UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Monitoring, estimation, and robust control of microgrids for safe operation

by Hamidreza Shafei - [redacted]

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

under the supervision of
A/Prof. Li Li
A/Prof. Ricardo P. Aguilera
Dr. Hassan Haes Alhelou

University of Technology Sydney
Faculty of Engineering and IT

July 2025

Certificate of Authorship/Originality

I, Hamidreza Shafei, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Electrical and Data Engineering at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature:

Production Note:
Signature removed prior to publication.

Date: July 14, 2025

Dedication

To my beloved parents.

Acknowledgment

I would like to express my sincere thanks to my supervisor, Prof. Li Li, whose unwavering enthusiasm for research sparked a spirit of exploration in my academic journey. I deeply value his enduring patience, thoughtful advice, and the considerable time he dedicated to guiding and reviewing my work. His mentorship has left a lasting impact that I will always remember.

Also, I would like to thank to Prof. Ricardo Aguilera and Dr. Hassan Haes Alhelou for their valuable insights and support during my PhD studies.

I'm grateful to my friend, Dr. Majid Farhangi, who continuously helped me in this path.

Finally, none of this would be made possible without the endless support of my family.

ABSTRACT

To meet the growing global energy demand, microgrids (MGs) have gained significant attention due to their numerous advantages. However, ensuring safe operation remains the foremost requirement for MGs, even during contingencies. MGs must function safely in both islanded and grid-connected modes, even when exposed to intentional or unintentional disruptive events. These events may stem from factors such as equipment failures, extreme weather conditions, sudden changes in load demand, noise, or cyber-attacks, all of which can negatively impact the safety, resilience, and reliability of MGs. While noise and fault signals are typically bounded, cyber-attacks pose a unique and critical threat as they are deliberately engineered to maximize damage and are not inherently constrained. Thus, ensuring the safe operation of MGs in the face of cyber-attacks has become a rapidly expanding area of research, presenting significant challenges in both detection and control strategies that remain to be addressed. Among all kinds of attacks, false data injection attacks (FDIAs) are deliberately crafted by intelligent adversaries to mimic normal system behavior, making them difficult to detect using conventional methods. Unlike natural disturbances, which are random and bounded by physical laws, FDI attacks are unconstrained and can be targeted to manipulate system dynamics and cause instability without triggering alarms. This thesis presents novel observer-based cyberattack-resilient control and operation methods for both dc and ac MGs, designed to enhance cybersecurity against FDI attacks. To effectively detect cyber-attacks targeting communication channels, two advanced model-based techniques have been developed: sliding mode and projection operator-based observers, both capable of attack reconstruction under unknown inputs. Since the proposed observers estimate the states of neighboring units without full access to their internal information, unknown input observers (UIOs) are employed to accurately reconstruct attacks under limited system knowledge. In this regard, each DG unit is equipped with a bank of these observers to estimate the dynamic states of all neighboring units. The developed attack reconstruction methods are integrated into a robust control and operation framework, designed to be resilient against cyber-attacks and focused on mitigating the harmful effects of FDIAs. Extensive real-time numerical simulations are conducted to evaluate the practicality and efficiency of the proposed approach under various attack scenarios. The results demonstrate its superiority over existing

methods by reducing overshoot by 21.43%, achieving a slightly faster settling time, and significantly improving the rise time by 83.95%.

Keywords: Microgrid, Cybersecurity, Attack reconstruction, Attack mitigation, Unknown input observer

Contents

List of Figures

List of Tables

List of Publications

Journal papers:

1. **H. Shafei**, M. Farhangi, L. Li, R.P. Aguilera, and H. Haes Alhelou, "A Novel Cyberattack Detection and Mitigation for Coupled Power and Information Networks in Microgrids Using Distributed Sliding Mode Unknown Input Observer," *IEEE Transactions on Smart Grid*, Early Access, 2024.

2. **H. Shafei**, M. Farhangi, S.K. Sarker, L. Li, R.P. Aguilera, and H. Haes Alhelou, A Distributed Projection Operator-Based Unknown Input Observer for Attack Detection and Mitigation on DC Microgrids, *IEEE Transaction on Cybernetics*, **Under revision**.

3. **H. Shafei**, S.K. Sarker, M. Farhangi, L. Li, R.P. Aguilera, and H. Haes Alhelou, Cyberattack Reconstruction and Mitigation with a Reduced-Order Unknown Input Observer-Based Approach for AC Microgrids, *IEEE Transaction ...*, **Under preparation**.

Book Chapter:

1. **H. Shafei**, L. Li, R.P. Aguilera, "A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems", In: Haes Alhelou, H., Hatziargyriou, N., Dong, Z.Y. (eds), Power Systems Cybersecurity: Methods, Concepts, and Best Practices, Springer Cham, 1-45. ISBN: 978-3-031-20362-6, 2023.

Conference papers:

1. **H. Shafei**, L. Li, and R.P. Aguilera, 2023, June. Observer-based Attack Detection and Mitigation in DC Microgrid Systems. In 2023 IEEE 14th International Symposium on Power Electronics for Distributed Generation Systems (PEDG) (pp. 959-964). IEEE.

2. **H. Shafei**, S.K. Sarker, L. Li, R.P. Aguilera, and H. Haes Alhelou, 2024, November. Innovative Observer-Based Framework for Attack Reconstruction and Mitigation in AC Microgrids. In 2024 IEEE 34th Australasian Universities Power Engineering Conference (AUPEC) (pp. 1-6). IEEE.

Related/Collaborative Publications:

Journal papers:

1. S.K. Sarker, **H. Shafei**, L. Li, R.P. Aguilera, and M.J. Hossain, "A DC Microgrid Cyber-Attack Detection and Mitigation Strategy Based on Bayesian Inference Dynamic Data-Driven Network", *IEEE Transaction on Cybernetics*, **Under review**.

2. S.K. Sarker, **H. Shafei**, L. Li, R.P. Aguilera, and M.J. Hossain, "Microgrids Cyber-security: Emerging Research Issues, Practices, and Progresses on Data-driven Techniques", *Energy Strategy Reviews*, **Under review**.

Conference papers:

1. S.K. Sarker, **H. Shafei**, T. Shi, L. Li, M.J. Hossain, and R.P. Aguilera, 2024, November. A Data-driven Multivariable Adaptive Cybersecurity Framework for Isolated Microgrids. In 2024 IEEE 34th Australasian Universities Power Engineering Conference (AUPEC) (pp. 1-6). IEEE.

Chapter 1

Introduction

1.1 Background and motivation

The global energy market is increasingly prioritizing renewable energy resources (DERs), reflecting a strong focus on sustainable power generation with reduced carbon emissions. Australia, like Europe, has outlined ambitious plans to expand its reliance on renewable energy and lower its carbon emissions. By 2030, the Australian government aims to generate 82% of its electricity from renewable sources [4,5]. At present, approximately 32% of Australia's electricity is derived from renewable resources such as wind, solar, and hydropower [6]. Furthermore, the country has pledged to cut greenhouse gas emissions by 43% compared to 2005 levels by 2030 and is working toward achieving net zero emissions by 2050 [7].

Based on the modern energy communities requirements, microgrids (MGs) are introduced to provide economical and reliable and provide environmental benefits [8]. Compared to traditional power grids, MGs offer more efficient operation with less pollution and higher power quality. According to [9], the amount of electricity needed worldwide is growing by 2.5% each year and power systems around the globe are going through the energy transition towards almost 100% renewable energy integration. This means that the traditional large fossil-based power plants are being replaced with distributed generating units (DGs) mainly placed on the demand side and integrated through the distribution grid. This enforces upgrading the existing power systems towards smart distribution grids built based on the integration of clusters of MGs powered by environmentally friendly DGs. Owing to their unique features, such as being easily accessible, efficient, and quick to set up, MGs have become a practical solution to several technical challenges and backbone in the future decarbonised energy systems in today's world.

With respect to the increase of energy consumption due to population growth, infrastructure and the energy-intensive technologies development, MGs have been a promising solution for today's

growing energy demand. An MG combines different DERs, energy storage systems, and various electric devices that provide energy for different applications. As they become more widely used and increasingly dependent on communication networks for control and management, the risk of cyber-attacks has grown considerably [10, 11]. Since these networks rely heavily on information and communication technologies, they are vulnerable to cyber threats, which can compromise the security, stability, and efficiency of power systems. Thus, cybersecurity for MGs has emerged as one of the primary challenges facing the power industry [12]. Considering the importance of providing cybersecurity for MGs, it has been the subject of various studies in the recent years to prevent their performance degradation resulting from cyber-attacks.

An MG typically consists of three layers: a) physical, b) control, and c) communication layers [13]. Physical layer includes devices like DERs, power converters, capacitors, and resistors, which are interconnected through power lines. Control layer comprised of primary and secondary control systems. This layer ensures that the MG meets its objectives. For dc MGs, the focus is on voltage regulation and proportional current sharing, while for ac MGs, voltage/frequency regulation and proportional active/reactive power sharing are targeted. Considering the communication layer, it oversees the interaction between DGs and the upstream grid. It is also a target for intrusions, as attackers may attempt to disrupt the entire MG. The growing adoption and utilization of MGs present the opportunities to develop robust and effective detection schemes, ensuring the secure operation of these systems against emerging and sophisticated attacks.

As mentioned above, the increasing integration of digital communication in MGs has heightened the risk of cyber-attacks. Cyber-attacks pose a significant threat to the safe and reliable operation of microgrids by targeting their communication, control, and monitoring infrastructures. Such attacks can lead to the manipulation or loss of critical data, unauthorized control actions, or denial of service, which in turn disrupt key control objectives such as voltage and frequency regulation, power sharing, and protection coordination. The resulting consequences may include system instability, degraded performance, unsafe operating conditions, and even large-scale outages—ultimately compromising the security, reliability, and resilience of the microgrid. There are a large number of cyber-attacks that have been occurred in the recent years. For instance, the 2015 cyber-attack on Ukraine's power grid, attributed to the Industroyer malware, demonstrated the potential for significant disruptions

caused by cyber threats [14]. In January 2003, intruders attacked the Dacis-Besse power plant in Oak Harbour (Ohio State, USA) with a slammer worm and shut down its safety display system [15]. In 2010, a malicious computer worm, known as the Stuxnet virus, targeted the supervisory control and data acquisition (SCADA) system of the Natanz nuclear site in Iran and caused serious damage to numerous nuclear centrifuges [16]. In 2011, the SCADA system at an Illinois water plant was breached and, as a result, the supply pumps were disabled [17]. Such incidents underscore the importance of securing the communication layer within MGs. These examples, from a long list of cyber-attacks, clearly highlight the importance of studying and researching cyber-security issues related to MGs [18]. A complete list of cyber-attack events can be found in [19].

According to the literature, there are two key strategies to protect MGs against cyber-attacks [20]: i) attack detection approaches [2]; and ii) attack-resilient control schemes [21]. Each of these schemes have their own pros and cons, which will be discussed in depth in the next chapter. In the first scheme, after attack detection, a mitigation scheme is utilized to prevent the spread of destructive impacts of cyber-attacks [22]. A common approach to mitigating the effects of cyber-attacks involves isolating the compromised agents from the system. In most existing research using this approach, attack reconstruction is performed by transmitting the estimated signals, which could potentially create an entry point for new cyber-attacks. However, this strategy reduces network connectivity, ultimately affecting overall system performance. In contrast, the second approach improves the resilience of microgrids (MGs) against attacks through the implementation of a distributed attack-resilient control system [23]. Figure 1.1 depicts the framework of an MG in the presence of various kinds of cyber-attacks through different channels.

This research will focus on developing new attack detection schemes to provide safe operation of MGs against various cyber-attack signals. The outcomes of this project will be highly applicable to industrial settings, offering reliable and effective solutions for mitigating the impact of cyber-attacks. The main objectives of this research are outlined in the next section.

1.2 Problem statement and research objectives

The cybersecurity of MGs is still in its early stages of progress, making it a hot and important topic for researchers in this field. Securing the safe operation of dc and ac MGs against intentional and unintentional adverse factors – such as faults, external disturbance, noise, cyber-attack, and so on– is

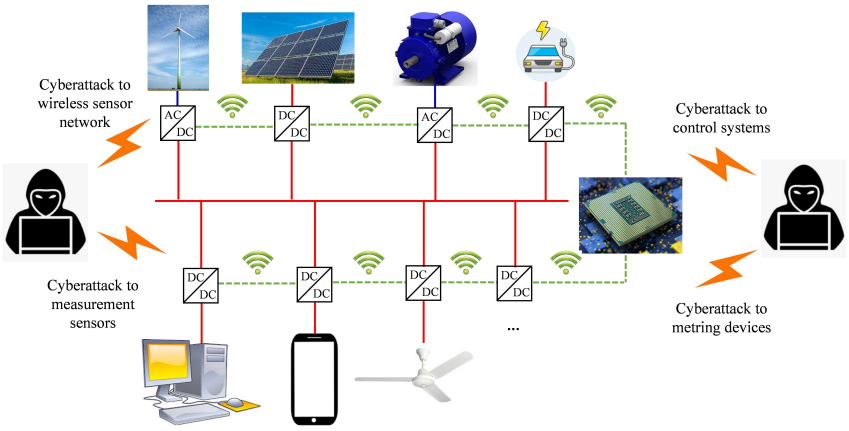


Figure 1.1 . The framework of an MG in the presence of various cyber-attacks

the primary objective of this work. In this regard, the main aim of this research is to propose observer-based methods to reconstruct and mitigate cyber-attacks on the DG communication channels. More specifically, this work develops unknown input observers to estimate the states of neighboring DGs without requiring access to all their inputs for attack detection purpose, which should be developed for both ac and dc MGs. By mitigating the effects of attacks, safe operation of dc/ac MGs can be provided. The specific research objectives of this thesis are outlined as follows:

1. Reconstructing false data injection attacks, as one of the most common types of attack, in dc and ac MGs with robust observer-based methods to countermeasure their destructive impacts.

2. Providing safe operation for dc and ac MGs without requiring additional information exchange, preventing the occurrence of new cyber-attacks.

3. Providing a mathematical stability proof of the proposed scheme to ensure its effectiveness against cyber-attacks.

4. Implementing the proposed scheme on real-time simulator to illustrate the ability of the proposed scheme against various scenarios, including constant, time-varying and unbounded, and fast cyber-attacks in real communication conditions.

5. Improving existing schemes for attack detection and mitigation through addressing existing

drawbacks, including knowing the upper bound of unknown inputs, which is a limiting factor, and transmitting additional information.

1.3 Thesis overview

The rest of the thesis is structured as follows:

Chapter 2 studies different types of cyber-attacks and their relevant mathematical expressions. In this chapter, a comprehensive literature review has been provided on the major aspects of cyber-security with a focus on model-based methods, which is the primary concern of this research. In addition, the existing research gaps in the literature are explained.

Chapter 3 aims to develop a robust sliding mode-based unknown input observer to estimate the states of neighboring units with the purpose of attack detection. This method is designed for dc MGs to make them immune against FDIAs. Moreover, by designing primary and secondary control systems, the main objective of dc MGs, that is, accurate voltage regulation and proportional current sharing between DG units, are achieved. In this chapter, by providing mathematical proof and divers real-time simulation results, the effectiveness of this scheme has been justified.

Chapter 4 aims to address the drawbacks of the developed SM-based unknown input observer (UIO) in the previous chapter with a projection operator-based UIO. In this regard, a new PO-based UIO is developed for dc MG to mitigate the impacts of cyber-attacks without requiring additional transmitted signals between DGs. In addition, a state feedback with an integral action control system is designed in the primary control level to secure the stability of the dc MG. In addition to mathematical proof, extensive real-time simulation results confirm the effectiveness of this scheme in dealing with FDIAs.

Chapter 5 develops the scheme presented in Chapter 4 for ac MGs. For this purpose, the dynamic equations of ac MGs have been augmented by considering attack signals in the active and reactive power channels. by designing primary and secondary control system, the desired objective of ac MGs, that is, accurate voltage and frequency regulation, and proportional active and reactive power sharing between DGs, have been achieved. Similarly, mathematical proof and various real-time simulation results are provided to show the efficacy of this scheme in dealing with FDIAs.

Finally, this work is concluded in Chapter 6, where the contributions of this thesis are summarized. Moreover, the future directions of this research to improve this research has been explained.

Chapter 2

Literature Review

This section presents a comprehensive survey of the research conducted so far in the field of cybersecurity in MGs. As mentioned in Chapter 1, there are two primary approaches to addressing cyber-attacks: 1) attack reconstruction and mitigation, and 2) the implementation of a resilient control system. This chapter studies both approaches, highlighting their advantages and limitations.

2.1 Various kinds of cyber-attacks

Thanks to the tremendous progress in communication technology, a fundamental revolution has occurred in cyber-physical systems (CPSs) [24]. Since becoming more distributed and network integrated, the CPSs have become more prone to cyber threats, and network anomalies [25]. As the complexity of CPSs increases, the potential impact of such attacks on system reliability and safety grows significantly, indicating the importance of more effective and reliable cyber-security schemes. Cyber-attacks occur mainly on two fronts: software and hardware. Software attacks generally lead to communication interference, manipulation, and communication latency, while hardware attacks cause physical damage to sensors or modify sensor information. Among these two types of attacks, hardware attacks are the most dangerous [26].

The first step to deal with cyber-attacks is to identify them. There are various kinds of cyber-attacks, each of which with particular goals and consequences. For example, some attacks may affect actuators and controllers, some may focus on sensors, some try to block transmission data channels, and others attempt to falsify the information signals. Cyber-attacks can target different channels of a CPS–such as actuators and sensors–and thus degrade the performance of MGs by adversely affecting one of their essential characteristics (i.e., availability, integrity, timeliness, and confidentiality of data). These features are critical to maintain the efficient and reliable operation of MGs.

Availability: Availability refers to the accessibility and availability of data at all times [27], which can be lost under attacks by denial of service (DoS).

Integrity: This feature requires the data to be clean and reliable. The process of generating, transmitting and storing data must be genuine and free of corruption [28]. The Replay and FDIAs may compromise the essential feature of data integrity.

Timeliness: This crucial feature concerns the processing, generation and availability of data in real time [29], which may be lost with replay attacks.

Confidentiality: Confidentiality indicates the availability of data only to authorized users [30], and could be adversely affected by Man-in-the-Middle (MITM) attacks.

The following sections have provided brief descriptions of different types of cyber-attacks, and their mathematical models. Due to the diversity of cyber-attacks, it is vital to know the characteristics of each one and to find practical means to mitigate their effects.

2.1.1 DoS attack

To disrupt the availability of data, potential intruders try to make communication networks inaccessible. Among various cyber-attacks, DoS attacks target this aspect of data, where it can be performed in two ways, flooding services or crashing services. In flood attacks, with the aim of slowing and eventually stopping the services, attackers send too much traffic for the server to buffer. In addition, it can occur by jamming signals to block communication channels. To this end, data from a sensor or actuator can be prevented from reaching their intended destination. Thus, a DoS attack on a sensor or actuator can be mathematically formulated with the following availability function [31]:

$$p(t) = \begin{cases} 1 & for\ t \in \Pi_N \\ 0 & for\ t \in \Pi_D \end{cases} \tag{2.1}$$

For DoS attacks, two time intervals must be taken into account: $\sigma_D = h_0, h_1, ..., h_k, ...$, representing the instances when a DoS attack occurs, and $\sigma_I = \tau_0, \tau_1, ..., \tau_k, ...$, indicating the duration of each DoS attack. Furthermore, $h_{k+1} - h_k > \tau_k > 0$ indicates that there is a normal communication period between two consecutive DoS attacks [32]. In the above equation, $\Pi_D(h,t)$ denotes all the time intervals in which DoS attacks occur over $[h,t)$, where $t > h$. On the contrary, $\Pi_N(h,t)$ represents all the time intervals in which there is a normal communication over $[h,t)$. It is clear that $\Pi_N(h,t) \cap \Pi_D(h,t) = \emptyset$ and $\Pi_N(h,t) \cup \Pi_D(h,t) = [h,t)$. In (2.1), $p(t) = 0$ means the presence of a

DoS attack and $p(t) = 1$ denotes the absence of a DoS attack. Fig. 2.1 depicts the structure of a DoS attack, where $x(t) \in R^n$, $u(t) \in R^m$, $y(t) \in R^p$, and $w(t) \in R^n$ are the state variables, control input, output signal, and process noise, respectively. This figure highlights both the system architecture and the temporal characteristics of the attack. Figure 2.1 (a) illustrates the closed-loop control structure, which includes the plant, actuator, controller, detector, and sensors. The DoS attack targets this network, specifically the communication links between the sensors and controller, and between the controller and actuator. When the attack is active, it blocks the transmission of measurement and control signals, effectively disrupting the feedback loop and limiting signal exchange to discrete time instants t_k, corresponding to periods when the network is available. Figure 2.1 (b) models the timing behavior of the DoS attack through a sequence of alternating active "On" and inactive "Off" intervals. During the "On" periods, represented in red, the attacker prevents data transmission, while during the "Off" periods, normal communication resumes. Each attack instance is defined by its starting time h_i and duration τ_i. This time-domain model is essential for evaluating the resilience of the control system and for designing detection and mitigation schemes capable of maintaining system stability and performance under intermittent communication disruptions caused by DoS attacks.

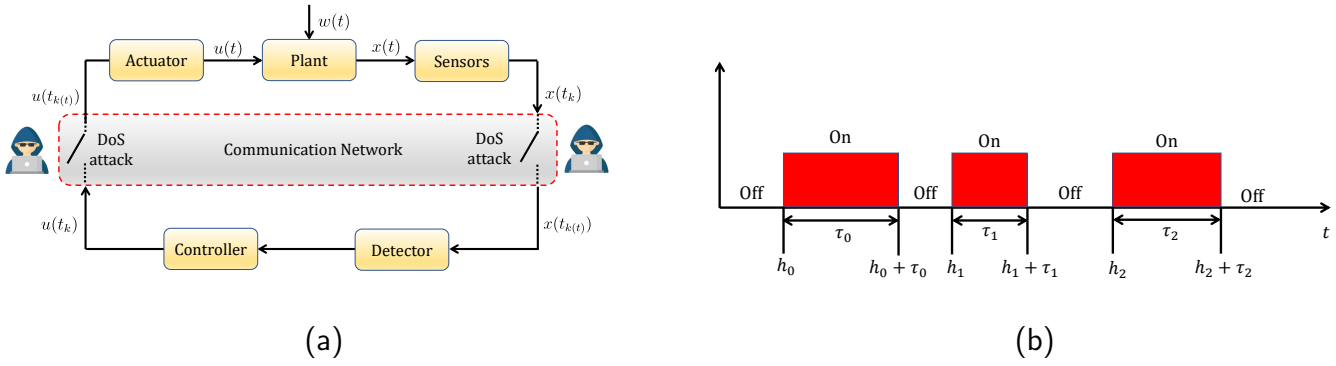


Figure 2.1 . **(a).** DoS attack representation and **(b).** Time intervals in DoS attack [1].

2.1.2 FDI attack

To destroy the data integrity, attackers try to alter the states of a system by injecting false data into sensors and actuators [33] [34]. FDIA is launched through sensor spoofing, intrusion of communication links, magnetic field injection attacks, GPS spoofing, and so on. In systems with unstable modes, FDIAs attempt to modify the system measurements so that some unstable system modes

become unobservable. FDIAs directly compromise key microgrid control objectives—such as voltage and frequency regulation, and proportional power sharing—by injecting false data into measurement signals or control commands. This manipulation can mislead controllers into making incorrect decisions, resulting in instability, power imbalances, and degraded overall system performance. Such attacks pose severe threats to system security, stability, and reliability by enabling undetected manipulation of critical control signals. If not promptly detected and mitigated, they can lead to loss of synchronism, equipment damage, and widespread service disruptions. Similar to DoS attacks, they can also be applied to both the actuator and the sensor channels, as follows [1]:

$$\begin{aligned} \tilde{u}_j(t) &= u_j(t) + a_{u_j}(t), \\ \tilde{y}_j(t) &= y_j(t) + a_{y_j}(t), \end{aligned} \tag{2.2}$$

where $\tilde{u}_j(t)$ and $\tilde{y}_j(t)$ are the disrupted control input and output signals, respectively. In this equation, $u_j(t)$ and $y_j(t)$ are the desired control input and measurement. In addition, $a_{u_j}(t)$ and $a_{y_j}(t)$ are the FDIA signals to the actuators and sensors, which are defined as follows:

$$a_{u_j}(t) = \begin{cases} 0 & \text{for } t \notin \tau_{a_j} \\ \lambda_j \mathcal{F}_j(.) & \text{for } t \in \tau_{a_j} \end{cases}, \; a_{y_j}(t) = \begin{cases} 0 & \text{for } t \notin \tau_{a_j} \\ \lambda_j \mathcal{F}_j(.) & \text{for } t \in \tau_{a_j} \end{cases} \tag{2.3}$$

In the above equations, τ_a is the attack time period and λ is an attack parameter. $\mathcal{F}$ can either be a time/state-dependent function or completely independent.

2.1.3 Replay attack

A replay cyber-attack targets the integrity of a system's data and timeliness features. This attack can occur practically through the monitoring and recording of sensor measurements during invasion. Then, attackers use them instead of the actual measurements. In this kind of attack, the attackers record a data sequence for a certain amount of time and then replay these readings in the system to deceive the operators. In replay attacks, the attackers do not need any information about the target system. This attack can be modeled as follows:

$$a_y(t) = -Cx(t) + y(t-\tau) \quad 0 < \tau < t \tag{2.4}$$

where $a_y(t)$ is the replay attack in the sensor channel. Furthermore, $x(t) \in R^n$ and $y(t-\tau) \in R^p$ are the state of the system and the sensor data collected through monitoring, respectively. This

procedure should consider two different stages: 1) the monitoring phase and 2) the replay phase. In the monitoring phase ($0 \leq t < t_0$), the collected measurements are stored in $J(t)$, and thus [1]

$$\begin{aligned} y_a(t) &= 0 \\ J(t) &= \Gamma^y \cdot y(t) \end{aligned} \tag{2.5}$$

In this phase, cyber-attack is not yet applied (i.e., $y_a(t) = 0$), while in the replay phase, the gathered data from the monitoring stage are sent to the controller. So, we have

$$\begin{aligned} y_a(t) &= J(t - t_0) \\ J(t) &= J(t - 1) \end{aligned} \tag{2.6}$$

The same procedure can be applied to model replay attacks in an actuator channel. Figure 2.2 depicts the structure of this type of attack, where u_a and y_a are the actuator and sensor attack signals, respectively. In addition, d is the external disturbance that acts on the plant and u is the infected control signal. The replay attack targets both the sensor-to-controller and controller-to-actuator communication links. On the control input path, the attacker injects a false control signal $u_a(t)$ into the system, which is combined with the original control command $u(t)$. Similarly, on the measurement path, the attacker replaces the true measurement $y(t)$ with a falsified version $y_a(t)$, which is typically a previously recorded sequence of legitimate measurements. These recorded signals are replayed to the controller at a later time, thereby concealing the actual system behavior and misleading the control system into operating under incorrect assumptions. Such an attack is particularly dangerous because it can be stealthy: the injected signals $y_a(t)$ and $u_a(t)$ may appear statistically identical to legitimate data, making it difficult for traditional anomaly detectors to recognize the intrusion. The attacker does not necessarily need detailed knowledge of the system model but can still cause significant performance degradation or instability by feeding outdated or incorrect information into the control loop.

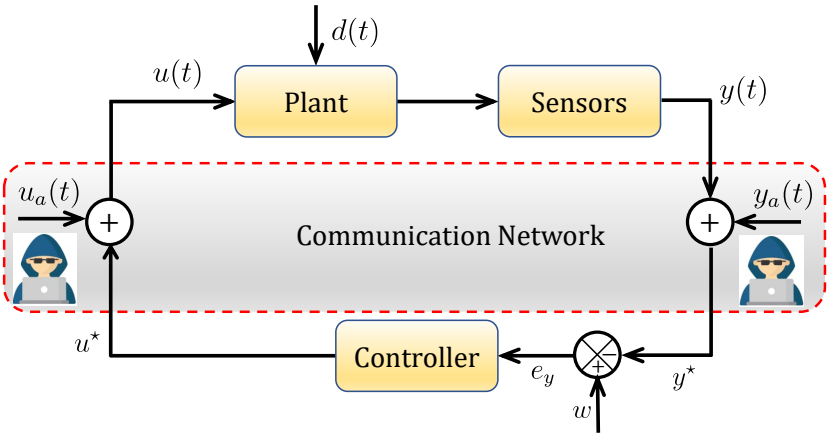


Figure 2.2 . Replay attack representation

2.1.4 Covert attack

The covert attack is another hard-to-detect cyber-attack in which the attackers modify the measurements of a system so that it cancels out all the effects of the attack on the system dynamics. To practically apply this kind of attack, attackers cancel the effect of attacks by calculating the system's output response and subtracting it from the measurement readings. In this type of attack, the attackers apparently have access to both the actuator and sensors. Therefore, complete knowledge of the system is required. To mathematically model the covert attack, the following two steps should be taken [35].

1. The actuator of the system is manipulated by the attackers as follows:

$$\tilde{u}_t = u_t + a_t, \tag{2.7}$$

where u_t is the original control law, a_t is the corrupted signal injected by attackers, and $\tilde{u}_t$ is the corrupted control signal which will alter the system states at time $t+1$, as follows:

$$\tilde{x}_{t+1} = x_t + Ba_t \tag{2.8}$$

As a result, the output signal changes to the following:

$$\tilde{y}_{t+1} = y_{t+1} + CBa_t \tag{2.9}$$

2. The sensor measurements are modified so that the attack cannot be detected. Thus,

$$\check{y}_{t+1} = \tilde{y}_{t+1} - \Upsilon \tag{2.10}$$

where $\Upsilon = CBa_t$. By doing so, the altered measurements (i.e., $\check{y}_{t+1}$) get to be exactly equal to the original measurements in the absence of an attack (i.e., y_{t+1}). Therefore, this kind of attack is disguised.

2.2 Attack detection and mitigation

As mentioned previously, detecting cyber-attacks through state observation and mitigating their harmful effects by correcting compromised signals is one of the effective approaches for addressing cyber-attacks in MGs. This chapter explores all techniques within this category, including model-based and data-based methods that have been developed for cybersecurity purposes in MGs. In the following sections, we review the methods used to address cybersecurity challenges in MGs.

2.2.1 Signal-based methods

Signal-based attack detection methods in MGs are implemented by monitoring communication link signals in real time. In this approach, any discrepancy between a system's states and its desired values is flagged as a potential attack [21]. Without relying on prior knowledge of system dynamics, Beg et al. [36] identified FDI and DoS attacks in complex dc MGs by employing a temporal signal logic formula and comparing system voltages and currents against pre-set thresholds. Similarly, in [34], a cooperative vulnerability factor is introduced to detect FDIAs in voltage measurements by monitoring secondary sub-layer outputs and tracking attack-induced changes. To pinpoint attacked nodes under an FDIA, a consensus algorithm based on discordant elements was proposed in [37]. In [38], a short-term state forecasting scheme is developed that combines norm and L residual measurement analysis to detect FDIAs by analyzing discrepancies between received and predicted measurements. Furthermore, Madichetty et al. [26] presented a low-computational approach using an adaptive state observer to estimate system currents and voltages under FDIAs. This method enables real-time detection of FDIAs by examining the error between the estimated and actual signals.

As a sub-branch of signal-based methods, the weighted least-square scheme is a reliable and efficient technique for attack detection in MGs [39]. Using the graph signal processing technique,

Drayer and Routtenberg [40] devised an attack detection scheme for ac MGs. By comparing the maximum norm of the graph Fourier transform of an estimated grid state with a predefined threshold, they could detect the presence of FDIAs. In this approach, the high-frequency components related to the large eigenvalues of the Laplacian matrix are filtered out. The same approach is also used to detect on data integrity and availability in power generation systems [41]. In another study, Basati et al. [42] proposed a supervised algorithm based on adaptive neuro-fuzzy inference systems to accurately monitor the voltages and currents of all DGs in real time. For FDIAs detection in dc MGs, all DGs' voltages and currents estimation values are compared with their actual values. The effectiveness and robustness of this signal-based technique for attack detection and mitigation have been validated with computer simulations. Zografopoulos et al. [43] developed an attack detector by identifying the stable kernel representation of the islanded MGs in the attack-free case. In this work, the proposed scheme was tested in the presence of three different cyberattacks on model input, system states, and measurement data to show its ability to detect various types of cyberattacks. Li et al. [44] developed a high-dimensional data-driven attack detection using electric waveform data. Using the data structure, this method does not need a training stage for attack detection, which can be considered one of its advantages.

One of the significant shortcomings of signal-based methods is that the relationship between measured data and control signal is not investigated, which is necessary for reliable detection [45]. Moreover, the limitations of such schemes in the detection of stealth attacks are mentioned in [46], which can be considered another drawback.

2.2.2 Model-based methods:

Another widely used approach to detect attacks in MGs is based on mathematical models. Common techniques in this category include observer-based methods that try to detect intruders by estimating the states of attacked systems. In the literature, there are several methods that have been developed for attack reconstruction purposes in MGs, including Kalman filter (KF) [47], sliding mode observer (SMO) schemes [48], UIOs [49], and so on. This section examines each of these schemes and outlines their strengths and limitations.

Kalman filter-based techniques

KF is a common scheme used for state estimation. This method can achieve an accurate state estimation by applying an optimal recursive algorithm and using the previously estimated states and the current measurements. Since previous measurements are not needed in this approach, it is considered an efficient state estimation strategy. KF method can be conducted in two steps: (a) the prediction step, and (b) the correction step [50].

Several filtering techniques have already been proposed for the estimation of dynamic states, such as the extended Kalman filter (EKF) [51], unscented Kalman filter (UKF) [52], and the cubature Kalman filter (CKF) [53]. For example, Manandhar et al. [22] used KF to estimate the state variables of a system. A χ^2 detector was then employed to utilize the estimated states and system readings to detect emerging system faults and various types of attacks. In another study, KF was applied to estimate the expected measurements, which were subsequently used to calculate the deviations between the actual and estimated values [54]. In this process, a Chi-square detector and the cosine similarity matching technique were applied to detect cyber-attacks. Sargolzaei et al. [55] developed a KF-based observer to estimate the states of a system. In order to accurately deal with FDI attacks, they proposed a neural network (NN) architecture, whose weights were updated via an EKF. In another study, a resilient detection and mitigation-based controller have been devised for load frequency control against FDIAs [56]. They proposed a Luenberger observer along with an artificial neural network (ANN) enhanced by an EKF for online anomaly detection. In [53], a robust CKF is employed to dynamically estimate the states of a system under both FDI and DoS attacks in real-time. In this work, the superiority of the robust CKF over the CKF is illustrated. A comparison between CKF and nonlinear observers was conducted in [57] to show the performance of each of these schemes in the dynamic estimation of system states in the presence of cyber-attacks and model uncertainties.

In another study, Adeli et al. [58] employed a trust-based UKF combined with a modified secure mode strategy to estimate the states of nonlinear systems under cyber-attacks. To prevent the spread of compromised data, a cluster-based fusion approach was developed. The limitations of the traditional KF in detecting stealth attacks were analyzed in. Using the upper bound of filtering error covariance minimization, a modified UKF was proposed in [59] for a specific class of nonlinear

systems under sensor saturation and randomly occurring FDIAs. This paper also provides sufficient conditions for the exponentially bounded filtering error. Using a KF decomposition framework, the secure estimation of system states for linear time-invariant Gaussian systems under sparse integrity attacks was achieved in [60]. Additionally, the study established sufficient conditions to ensure the stability of the proposed estimator.

In general, apart from the positive features of KF schemes in providing reasonable state estimation when the precise mathematical model of a system is available, the performance of KF-based methods deteriorates in the absence of a good model or the presence of external disturbances. In addition, the initial conditions of the considered states and covariance matrices can affect the estimation quality.

Sliding mode observer

A common method of state estimation in MGs is the SMO, which has intrinsic robustness against uncertainties, noise, and disturbances [61, 62, 63, 64, 65, 66, 67, 68]. In this approach, the system states are estimated in a finite time by forcing them toward a stable manifold in the presence of uncertainties and disturbances. Despite the positive characteristics of the SMO, including its simple implementation, disturbance rejection ability, and robustness, it suffers from chattering due to its high frequency switching around the sliding surface [69, 70]. In the following, we will review some research works on attack detection with SMO.

Saha et al. [61] proposed an SMO-based fault diagnosis technique to estimate sensor measurement errors arising from possible cyber-attacks or sensor faults in dc MGs. The estimated errors are used to initiate a mitigation action to ensure the operation of a resilient system. Most of the previously developed SMO-based methods assume a linear MG model, which is a restrictive assumption. In fact, in the presence of constant power loads (CPLs), the system linearity assumption will no longer be valid. In this regard, Cecilia et al. [2] proposed a distributed nonlinear observer that can robustly detect FDIAs in both the cyber links and the current sensors. In this work, the system equations were transformed into a form suitable for observer design purposes. To estimate the states of a system in the presence of a time delay, a sliding mode estimation-based control system was presented in [62], which estimates the states of an MG and predicts time delays. Furthermore, to ensure system stability and the accuracy of the estimated time delays, the estimation error was considered a disturbance to the sliding mode control (SMC) and used to update it adaptively. To estimate the

state of the system and detect sensor attacks, Ao et al. [63] proposed two adaptive SMOs, whose parameters are updated online. They also established sufficient conditions for attack detection.

In another study, Rinaldi et al. [64] proposed a distributed adaptive dual-layer super-twisting SMO to isolate, reconstruct and mitigate the adverse impacts of disturbances and communication attacks. In this paper, similar to [63], the observer gains are adjusted with an adaptive law. After reconstructing the attacks, a standard proportional integral (PI) controller is employed to mitigate their destructive effects. The same procedures have also been used for other types of SMO schemes, such as the integral SMO [71], the terminal SMO [72], and the high-order SMO [73]. To deal with cyber-attacks on sensors, an SMO was proposed in [68], which is sensitive to sensor attacks. This observer alerts the operators when at least one of the MGs is under sensor attack. Furthermore, another SMO is proposed to isolate the exact compromised subsystem, which is sensitive to attack on the i-th sensor but robust against external disturbances and sensor attacks other than those on the i-th agent. In another work, an SMO-based state and attack reconstruction scheme with the system augmentation and linear matrix inequality (LMI) approach is presented to detect FDIAs in both the sensor and actuator channels [74].

Li et al. [75] investigated an augmented state observer that uses a terminal integral adaptive SMC to estimate the system states under FDIAs to sensors and actuators. Su et al. [66] modeled MGs under dynamic load-altering attacks and developed a robust SMO that generates a residual signal. Cyber-attacks are then detected by comparing this signal with a threshold value. In [76], an SMO with adaptive parameters was explored that uses an equivalent output error injection algorithm to estimate system states and reconstruct sensor faults in the presence of incorrect information about scheduling parameters. Taking into account the unknown inputs and the sensor attacks, a linear discrete-time state-space and a sparse vector were devised to model the system and the cyber-attacks, respectively [67]. A new model in the descriptor form that uses an iterative approach was developed to estimate the state of the system under unknown inputs. This model proposes a novel sparse SMO that employs a projection operator for estimating the system states affected by cyber-attacks.

The weakness of SMO-based methods in detecting intelligent attacks with changing distributions can be considered a drawback. Furthermore, in the presence of unknown disturbances in the system (e.g., voltage oscillations, load variations, and neighboring voltage variations), these methods may

need to be revised to achieve a reliable state estimation [77]. Table 2.1 summarizes some of the recently published works in cybersecurity with model-based schemes.

Unknown input observer

As mentioned above, observer-based approaches, particularly UIOs, are among the most widely adopted techniques for FDIA detection and mitigation in model-based methodologies [85]. UIOs are a specialized class of observers designed to estimate the state variables of a system in scenarios where certain input signals are unknown or unmeasurable. This capability makes UIOs highly valuable for attack detection in MGs, particularly in situations where inputs to neighboring units are unavailable. These observers work by decoupling the system state estimation from unknown inputs, enabling accurate state reconstruction despite these uncertainties. Thanks to its unique features, this approach has attracted high attention in the cybersecurity of MGs [86,87]. For example, in [49], a distributed UIO is designed to identify cyberattacks and malfunctioning measurement units within interconnected power networks. To mitigate the effect of cyberattacks, operators need to replace compromised measurement data with the corresponding estimated values. Similarly, a set of UIOs combined with a Luenberger observer has been introduced to detect FDIA in MGs [88]. This method emphasizes attack detection while presuming that communication channels operate under ideal conditions. In another work, an SMC-based UIO is proposed to reconstruct FDIAs in load frequency control systems with unknown inputs [89].

Recently, a bank of SMO-based UIOs is proposed for attack reconstruction in MGs, under the assumption that certain signals are transmitted through secure channels, a constraint that may limit the applicability of the model in broader settings [87]. In another work, a UIO-based attack reconstruction method is introduced which overlooks the effects of noise and uncertainties. Additionally, this approach has a limitation on the number of sensors that can be affected by attack signals [90]. In [91], a bank of observers is designed for attack detection in dc MGs, with the primary limitation being the assumption of secure channels for some data transmission. An UIO was developed in [92] to detect the compromised agents in a distributed manner. In this study, the attacked signal was considered as an external input with no prior information. Then, sufficient and necessary conditions for observing the system's misbehaviors were established. Barboni et al. [83] proposed a distributed UIO-based scheme to detect covert attacks on large-scale interconnected systems. By augmenting

Table 2.1 . A brief review of the attack detection and mitigation studies using the model-based approach.

No	Study	Year	Attack type	Method	Advantages	Disadvantages
1	Saha et al. [61]	2018	FDI & Replay attack	Using a SMO to detect attacks	Presenting a complete model of MGs Considering its effectiveness against different situations	Just bounded attacks Required the exact model
2	Abianeh et al. [78]	2021	FDIAs	With localized communication link quality observer & multi-objective SMC	Able to deal with unbounded & extreme attacks, Low vulnerability to FDIAs & time delay is low	Strongly model-dependent, just for FDIAs.
3	Shi et al. [79] & Li et al. [80]	2021	FDIAs	Adaptive distributed observer	Low vulnerability to FDIAs, High reliability and robustness to cyberattacks	Vulnerable to time delays
4	Sahoo et al. [81]	2021	FDIAs	Using localized observer	Detecting other kinds of cyber-attacks	Vulnerable to time delay.
5	Li et al. [53]	2019	FDI & DoS attacks	Robust Cubature KF	Dynamic state estimation against FDA & DoS	Validated with a simple system
6	Afshari et al. [82]	2020	Time-varying & unbounded Deception attack	Using distributed state observer (DSO) to estimate the states and attack signals	Considering battery effects Able to deal with unbounded attacks.	Just for AC MGs & deception attacks.
7	Barboni et al. [83]	2020	Covert attacks	Robust model-based observer	Developing robust distributed observers Applicable to large-scale systems	Just bounded attacks Dependant to model accuracy
8	Poudel et al. [84]	2020	FDIAs	Distributed Kullback-Liebler observer	Determining the reliability and trustworthiness of the information.	Exact model is needed.
9	Cecilia et al. [48]	2021	FDIAs and Uncertainties	Extended Astolfi/Marconi plus linear Luenberger observers	Able to estimate unobservable states	Not applicable to other attacks.
10	Cecilia et al. [2]	2021	FDIAs and Uncertainties	High-order SMO along with a nonlinear open loop observer	Distributed HOSMO design for unobservable states under FDIAs and CPL conditions.	Relies to open-loop integration (Not tunable)
11	Sahoo et al. [34]	2019	FDIs and Stealth attack	Using cooperative vulnerability factor framework	Stealth attack detection. CVF factor to alarm the attacked agents.	Just applicable to AC MGs.
12	Yan et al. [62]	2017	Time delay	Estimation error used as a disturbance in SMO	Considering several kinds of delays and attacks	Exact model is required.
13	Manandhar et al. [22]	2014	DoS	KF with X2 detector	Resilient to spoof attacks low computational complexity	Model dependant Vulnerable to disturbances

the original system with a switched auxiliary one, the covert attacks were detected via a switched Luenberger observer. In another study, an unknown input interval-based observer was proposed to address biased load attacks by mitigating the effects of regionally interconnected information and disturbances [93]. Additionally, a novel detection criterion was introduced to overcome the limitations of previous threshold-based approaches. To better highlight the contribution of the recently published works, Table 2.2 is provided, in which a comparison between UIO-based methods has been conducted. The reviewed articles highlight a significant drawback in the transmission of estimated signals between neighbors. With this technique, the states of all neighboring units can be locally estimated within each DG, effectively preventing the risk of new cyber-attacks that could arise from signal transmission between neighbors.

Thanks to its unique features, this approach has attracted high attention in cybersecurity of MGs [94, 86, 87, 95]. For instance, in [49], a distributed UIO is designed to identify cyber-attacks and malfunctioning measurement units within interconnected power networks. To mitigate the effect of cyber-attacks, operators need to replace compromised measurement data with the corresponding estimated values. Similarly, a set of UIOs combined with a Luenberger observer has been introduced to detect FDIA in dc MGs [88]. This method emphasizes attack detection while presuming that communication channels operate under ideal conditions. To improve the accuracy of physical state estimation, a UIO-based detection method against FDI attacks was presented [94]. In another study, a bank of SMO-based UIOs is proposed for attack reconstruction in dc MGs, under the assumption that certain signals are transmitted through secure channels—a constraint that may limit the model's applicability in broader settings [87]. In another study, resilient control of cyber-physical systems under cyber-attacks is addressed by proposing a finite-time extended state observer based on the supertwisting sliding-mode algorithm to estimate system states and lumped uncertainties in the presence of actuator attacks [96]. A composite finite-time resilient controller is then developed, combining global fast terminal sliding-mode control with prescribed performance control. However, this methodology relies on secure communication channels for transmitting signals. In [97], a detection-triggered recursive impact mitigation scheme is proposed to address secondary FDIAs in cyber-physical microgrids. The method combines anomaly detection with iterative mitigation updates to suppress the disruptive effects of stealthy FDIAs while preserving system stability; how-

ever, it requires additional current sensors to observe voltage bias injections. The reviewed articles highlight a significant drawback in the transmission of estimated signals between neighbors, which is addressed in this study. Furthermore, most previous researches assume that the interactions between each DG and its neighbors, along with local load conditions, are known. In reality, however, these factors are often unknown. This study overcomes these restrictive assumptions by treating these factors as unknown inputs. Consequently, the states of all neighbors are locally estimated within each DG, effectively preventing the risk of new cyber-attacks that could emerge from signal transmission between neighbors.

Other observer-based methods

As mentioned above, the observer-based state estimation and attack detection schemes usually use a deterministic state–space model of the system. A few examples of wide-ranging observer-based methods include the high-gain observers [99], Kullback-Liebler (KL) observer [100], and so on. These observers have been widely explored and used in various studies and applications.

Mustafa et al. [101] developed an attack detection scheme based on KL divergence criterion for ac MGs. The KL divergence factors were then used to mitigate the effects of cyber-attacks by determining the trustworthiness of the information received from other agents. Moreover, to inform other agents about the reliability of the transmitted data, each agent generates a self-belief factor and communicates it with their neighbors. By comparing the KL criteria for both the healthy and the attacked systems, the FDIAs on MGs can be detected [102]. The same approach has been employed to detect attacks on dc MGs in [84]. To secure the CPSs from periodic DoS attacks in both measurement and control channels, an $\mathcal{H}_\infty$ observer-based output feedback controller was developed in [103]. In this paper, considering DoS attacks with a cyclic dwell-time switching characteristic, an augmented system is achieved as a discrete-time cyclic dwell-time switched system with unstable and stable subsystems. The proposed observer-based controller is developed in a piecewise linear form for the resulting augmented system. Attack detection and mitigation by a finite-time convergent observer-based output feedback controller were also investigated in [104]. In this paper, two different cases are considered: a) when all the sensors are under attack, and b) when some of the sensors are attacked. The applied sensor attacks are reconstructed by using the proposed observer with adaptive gains. In this procedure, the corrupted measured outputs are cleared from the malicious content, and

Table 2.2 . A brief review of the attack detection and mitigation studies using UIO approach.

No	Study	Attack type	Method	Advantages	Disadvantages
1	Haes Alhelou et al. [49] - (2022)	Constant FDIAs	Unknown input-based observer	1- Detecting faulty measurement devices, 2- Handling unknown inputs	1- Ignoring attack mitigation, 2- Inability to handle other attacks 3- Need for a secure channel.
2	Gallo et al. [88] - (2020)	Constant FDI & Replay attacks	A bank of UIOs & Luenberger-like observer	1- Considering different attack types, 2- No need for a secure channel	1- Ignoring attack mitigation, 2- Considering ideal communication
3	Wu et al. [67] - (2018)	FDIA to sensors	SMO-based attack detection via an projection operator scheme	Dealing with unknown inputs	1- Complexity of proposed method 2- Ignoring attack mitigation, 3- Transmitting the estimated signals
4	Barboni et al. [83] - (2020)	Covert attack	Luenberger with UIOs	No need for a secure channel and extra information	1- Limited to just 1 attack in each DG, 2- No attack mitigation, 3- Ignoring parameter uncertainties
5	Liu et al. [98] - (2023)	Dynamic FDIAs & Zero trace stealthy	A bank of UIOs in each unit	1- Considering unknown inputs 2- No need for extra information	1- Attack is applied to 1 channel, 2- Transmitting the estimated states, 3- Not accurate attack detection.
6	Syrmakesis et al. [89] - (2023)	Constant FDIAs	SMO with an adaptive threshold	1- Considering uncertainties, noise, time-delay, and nonlinearities, 2- No need for extra information	1- Attack mitigation is ignored, 2- Unable to deal with other attacks
7	Liu et al. [97] - (2024)	Bounded time-varying FDIAs	UIO-based attack detection	1- Considering load conditions & couplings with neighbors as unknown inputs. 2- Using a cost-effective current sensor deployment.	1- Requiring to install additional current sensors on power lines.
8	Shafei et al. [87] - (2024)	Bounded and time-varying FDIAs	Distributed SMO-based UIO	1- Considering local load conditions and couplings with neighbors as unknown inputs. 2- Low computation complexity	1- Requiring a secured channel for attack detection, 2- The upper bound of attacks should be known.
9	Liu et al. [90] - (2024)	FIDAs to sensors	UIO-based attack detection	1- No need for a secure channel, 2- The ineffectiveness of unknown inputs in observer design	1- Limitation on number of polluted sensors, 2- Ignoring the impacts of uncertainties and noise.

the output feedback controller uses these cleaned signals to mitigate the impacts of cyber-attacks.

Anomalies in multi-agent systems (MASs) caused by both FDIAs on communication links and physical faults in their facilities were detected by solving a robust $\mathcal{H}_\infty$ multi-objective optimization problem and employing an independent and cooperative detector [105]. This approach achieved a balance between robustness to disturbances and sensitivity to attacks. In another study, Das and Madichetty [106] developed a Luenberger observer to estimate the current of a dc-dc converter based on its input voltage. This approach offers several advantages, including reduced sensor requirements, lower computational burden, and enhanced performance. Gao et al. [107] developed a novel observer with a set of K-filters to detect deceptive cyber-attacks in the sensor and actuator channels of a high-order nonlinear CPS. To detect cyber-attacks in the presence of disturbances and measurement noise, Yan et al. [108] proposed a novel FDIA detection scheme. This approach involved decomposing a large-scale MG into multiple interconnected subsystems and designing dynamic reduced-order observers to generate residual signals. These residuals were then compared against adaptive detection thresholds based on a prescribed performance benchmark.

The bias load injection attack (BLIA) is a type of FDIAs that specifically targets vulnerable generator loads. Given the destructive impact of BLIAs on MGs, developing a secure detection and mitigation strategy is crucial. To address this, a three-stage approach is proposed for BLIA detection in [86]. First, a subregion division technique is applied to reduce the complexity of attack detection in large-scale grid systems. Next, a robust adaptive detection method is employed to accurately estimate the system's physical dynamics. Finally, a logical judgment matrix is introduced to address the undetectability of sensor attacks under system vulnerabilities. To estimate the states of continuous time-invariant linear systems under sparse sensor attacks, An et al. [109] developed a supervisory state observer. This approach utilizes a bank of candidate nonlinear sub-observers combined with a switching logic. A monitoring function is employed to dynamically select the active sub-observer at each moment. In another study, Yang et al. [110] investigated the estimation of distributed states in large-scale power systems under both FDI and DoS attacks using a neighborhood coordination scheme. In this approach, DoS attacks are mitigated through a measurement predictor, while FDIAs are handled as measurement uncertainties."

2.2.3 Data-based methods

As mentioned above, model-based detection methods have the limitation of requiring an exact mathematical model of the system. To address this challenge, researchers have proposed data-driven techniques. Data-driven detection methods often use machine learning or statistical techniques to derive a system model from historical data and measurement signals [45]. Several popular intelligent cybersecurity approaches, including deep reinforcement learning, deep transfer learning, and generative adversarial networks, have been thoroughly explored in [111]. These methods can be categorized into unsupervised, semi-supervised, supervised, and reinforcement learning schemes.

Several studies have been conducted on data-based schemes for cybersecurity in MGs. For example, Ozay et al. [112] analysed the performances of supervised, semi-supervised, and online learning algorithms for FDIA detection on MGs. Habibi et al. [113] developed an intelligent-based method to detect FDIAs and identify the attacked agents in dc MGs. They proposed a time-series analysis and a nonlinear auto-regressive NN-based exogenous model to estimate dc currents and voltages. These researchers proposed a model predictive control (MPC)/ANN scheme for FDIA detection in another article [114], where an MPC plays the role of attack mitigator. Simultaneously, an ANN detects the FDIAs on dc MGs. In [115], an artificial intelligent method with a nonlinear autoregressive exogenous technique is proposed to detect FDIAs on voltage and current sensors. This method suffers from a large computational burden in real-time implementations. In another study, Wan et al. [116] used a data-driven attack detection for islanded dc MGs with a reinforcement learning algorithm, where a discordant detection method is used to detect intelligent cyber-attacks.

He et al. [117] proposed a deep learning framework based on convolutional neural networks to detect injected data measurements. This framework monitors both data measurements and network-level features. Experimental results demonstrated its strong performance, high accuracy, and low computational complexity. To detect FDIAs in the measurement channels, a long short-term memory recurrent NN technique is developed in [118]. Yousefi-Azar et al. [119] developed a learning technique based on an autoencoder network to classify and detect network attacks and anomalies. To address emerging types of cyber-attacks, self-adaptive attack detection techniques have been developed. In this regard, Zhang et al. [120] proposed a cyber-attack detection scheme based on deep belief network and genetic algorithm (GA). In this work, the optimal numbers of the hidden layers and neurons are

adaptively determined by the GA to enhance the attack detection precision. Moreover, the support vector machine (SVM) approach can be utilized for attack detection in high-dimensional spaces by constructing a series of hyperplanes using SVM learning datasets. In this regard, two machine-learning-based methods (i.e., supervised anomaly detection and the unsupervised distributed SVM) have been proposed to detect stealth attacks in ac MGs [121].

To address the limitations of conventional methods in balancing high accuracy with a low false positive rate for new and unknown attacks, a deep reinforcement learning (DRL)-based adaptive attack detection algorithm was proposed in [122]. Raman et al. [123] proposed an adaptive and robust attack detection method that utilizes a hypergraph-based GA for parameter selection and applies the SVM technique for feature extraction. Ma et al. [124] demonstrated that a resilient neuroadaptive dynamic control technique, based on the Gaussian radial basis function neural network (RBFNN), can ensure the semi-global uniformity and ultimate boundedness of all signals under various challenges, including FDI and DoS attacks, unknown control gains, system uncertainties, and output constraints. Additionally, Gaggero et al. [125] developed a NN architecture, specifically an autoencoder, to detect cyberattacks in battery energy storage systems. Simulation results indicated the effectiveness of this method over the SVM algorithm. In another work, Pourfard et al. [126] proposed an unsupervised attack detection method based on a Fuzzy c-means clustering scheme to identify FDIAs. To facilitate attack localization following topology reconfigurations, they introduced a technique that identifies attacks using probability distributions of system states.

Despite the advantages of these intelligent methods, they are burdened by heavy computational demands, making them unsuitable for large-scale distributed MGs. Table 2.3 provides a summary of various learning schemes employed for cybersecurity purposes, along with their respective advantages and disadvantages.

2.3 Resilient control system

Despite the many advantages of distributed control systems, such as enhanced flexibility, scalability, low communication burden, and faster system response, their vulnerability to cyber-attacks remains a significant challenge that must be fully addressed. As a result, cybersecurity has become more critical than ever [132]. Given the devastating consequences of recent cyber-attacks, cybersecurity, along with attack detection and mitigation, has achieved significant attention from researchers in

Table 2.3 . A brief review of the attack detection and mitigation studies using the model-based approach.

No	Study	Year	Attack type	Method	Advantages	Disadvantages
1	Habibi et al. [127]	2021	FDIAs	Artificial NN	Usable when all units are under FDIAs.	Coordinated FDIAs is undetectable
2	Habibi et al. [113]	2020	FDIAs	NARX NN	FDIAs detectable in current and voltage channels.	Strong database for training. Just constant FDIAs.
3	He et al. [117]	2017	FDIAs	Deep Belief Network	Resilient to FDIAs; suitable for large-dimensional systems	Computational complexity; Vulnerable to unforeseen attacks
4	Hughes et al. [128]	2022	DoS	Deep Reinforcement Learning	The system's model is not required; Suitable for complex problems	High computation cost, Requires faster technologies for training.
5	Kavousi et al. [129]	2021	FDIAs	Using "Prediction interval"	Accurate detection of FDIAs	High computational cost
6	Dehghani et al. [130]	2021	Constant FDIAs	Wavelet Singular Values	Using Gray Wolf to detect FDIAs Precise FDIA detection	Not suitable for real-time implementation
7	Gao et al. [131]	2020	Malware threats	Semi-supervised Recurrent NN	Increased training speed; Efficiency and precision	Needs optimization for classification.

the power industry. Due to the various sources of uncertainties (e.g., the plug-and-play functionality of DGs, changes in MG topology, and uncertain or unknown dynamics), resilient control systems are essential for managing MGs. In the presence of uncertainties and cyber-attacks, resilient controllers can offer benefits such as bounded control signals, reference tracking with zero steady-state error, and an acceptable transient response [133].

Resilient control of MGs has been achieved through various techniques, including SMC [134], adaptive control [135], robust $\mathcal{H}_\infty$ control [136], fuzzy control [137], and learning-based approaches [138]. For instance, Duan et al. [139] proposed a four-step attack-resilient distributed controller based on a detection-mitigation algorithm to protect dc MGs against data integrity attacks. Unlike grid-connected MGs, which primarily focus on achieving proper power-sharing among DGs, islanded MGs must ensure both fair power-sharing and accurate frequency and voltage regulation [140]. To address this, a cyber-attack-resilient distributed controller was proposed to handle time-varying and successive attack signals in communication links, local controllers, and master controllers. The method employs periodically intermittent communication to detect and isolate adversarial actions. Furthermore, consensus-based secondary control systems have been used to detect FDIAs in both dc [37] and ac MGs [81]. These methods detect cyber-attacks through an asynchrony index, a detection scheme that is highly dependent on the chosen threshold. In another study, Abhinav et al. [141] developed a resilient distributed secondary cooperative controller for islanded ac MGs in the presence of cyber-attacks. The performance of the proposed controller was evaluated under sensor and actuator attacks, as well as attacks on communication links. This study introduced a distributed observer-based controller to address sensor and actuator attacks, alongside a trust/confidence-based control system to mitigate the effects of cyber-attacks on communication links. Additionally, an attack detection scheme for partial primal-dual-based distributed frequency control was proposed in [142].

Although the terms "robustness" and "resilience" may seem similar, they refer to distinct characteristics in the context of power systems. Resilience pertains to a system's active response to unexpected and extreme events in real-time, whereas robustness refers to a controller's ability to maintain its desired performance passively in the presence of a defined range of disturbances. The detection and isolation schemes designed to enhance the resilience of control systems have certain

drawbacks: (a) they involve a trade-off between the timeliness of attack mitigation and the controller's robustness to normal disturbances when tuning the isolation criterion, and (b) the number of cyber-attacks that can be mitigated is limited [139]. Some studies have focused on improving the robustness of distributed control systems. For example, Ding et al. [143] proposed a distributed resilient secondary control system for a battery energy storage system under DoS attacks. To ensure robustness against DoS attacks, they applied an acknowledgment attack detection scheme and a communication recovery mechanism to restore the connectivity-paralyzed communication topology. By using the weighted mean subsequence reduced algorithm for each DER, corrupted information from neighboring agents could be discarded, ensuring the security of the proposed distributed secondary controller against FDI attacks [144].

A distributed resilient control system based on an adaptive technique was employed in [145] to restore the frequency and voltage of an ac MG, achieve fair real power-sharing, and balance the state-of-charge of multiple energy storage systems under abnormal conditions. To ensure the stability of an ac MG against unbounded attacks, Zou et al. [20] developed a fully distributed resilient controller for secondary frequency regulation and voltage containment by introducing a virtual resilient layer with hidden networks. However, they assumed that the hidden network to be secure, which may not be accurate in real-world applications. To address the cybersecurity in ac MGs, a resilient distributed optimal frequency control system using a leader-follower consensus protocol was proposed in [132], where a networked auxiliary system is integrated with the original control system. The resilience of MGs against infrastructure failures has been improved through a novel master-slave control system [146]. Baghaee et al. [147] proposed a decentralized, distributed, and robust mixed $\mathcal{H}_2/\mathcal{H}_\infty$ voltage control system for disturbance rejection and setpoint tracking. The linear matrix inequality (LMI) scheme was utilized to solve a multi-objective optimization problem, and a fuzzy logic approach was incorporated to enhance the controller's performance against nonlinear loads and minor/major disturbances. Additionally, Li et al. [148] introduced a resilient control system based on an adaptive control scheme for islanded ac MGs with communication links subjected to cyber-attacks. The proposed method's resilience in voltage and frequency restoration, along with its power-sharing capability, was validated through computer simulations.

Most research on resilient control systems addresses sensor and actuator attacks separately, often

using complex nonlinear models, which increases computational burden and complicates the analysis and control of attacked MGs. To address this issue, Zhao et al. [149] developed a resilient control system based on feedback linearization to handle both sensor and actuator attacks in MGs. By simplifying the mathematical model of the targeted MG, they implemented a hybrid resilient control scheme using adaptive terminal SMC. Additionally, a resilient cooperative output-regulated controller for heterogeneous linear MASs with unknown switching exosystem dynamics under DoS attacks was proposed in [150]. In this study, a distributed resilient observer was designed to estimate auxiliary states, and distributed controllers were developed for individual agents.

To guarantee the stable operation of the wind turbines in redistributing the generated power among the converters under the system faults and cyber-attacks, a resilient DC voltage controller was developed [151]. In another study, Sadabadi et al. [152] proposed a resilient controller that does not need any information about the nature or location of an attack. A Lyapunov-based approach and the graph theory were applied in this work to ensure average voltage regulation and proportional load sharing in the DC MGs affected by the FDIAs. To rectify the effects of sensor faults in the islanded MGs, Saha et al. [153] proposed an SMO integrated with an $\mathcal{H}_\infty$ output feedback control law. The purpose of designing the SMO was to estimate the sensor faults, which were then used to develop the proposed robust fault-tolerant controller. In another study, Sadabadi et al. [152] proposed a resilient controller that does not require prior knowledge about the nature or location of an attack. This work utilized a Lyapunov-based approach and graph theory to achieve average voltage regulation and proportional load sharing in dc MGs affected by FDIAs. Additionally, to mitigate the effects of sensor faults in islanded MGs, Saha et al. [153] proposed an SMO integrated with an $\mathcal{H}_\infty$ output feedback control law. The SMO was designed to estimate sensor faults, which were then utilized to develop the robust fault-tolerant controller.

A novel switching event-triggered resilient control scheme, combining droop control and MPC, was proposed at the primary control level to achieve frequency and voltage restoration, as well as power sharing in islanded MGs [154]. Additionally, a distributed consensus pinning-based control scheme was implemented at the secondary control level to address transient deviations and enhance response speed. To further improve the system's resilience against severe incidents, an integrated control technique combining both primary and secondary control levels was developed. In another

study, Vigneysh et al. [155] proposed a cascade two-degree-of-freedom controller, integrating a PI controller and an internal model controller, as a resilient control scheme to ensure the sustained operation of MGs under parametric uncertainties and unbalanced loads.

A summary of the resilient control schemes in the field of cyber-security, along with their merits and drawbacks, has been provided in Table 2.4.

1. Contrary to [2,49,156,157,158,67,159,98], one of the main challenges addressed in this thesis is preventing the transmission of estimated states for attack detection between neighboring DGs. This preventive measure aims to eliminate the risk of these transmissions serving as potential entry points for new cyber-attacks.

2. In [49,89,83,67,89], the literature rarely addresses a unified scheme capable of simultaneously detecting and remedying cyber-attacks across a wide range of types. However, such a scheme has been evaluated under different types of attacks in this thesis.

3. Similar to [49,88,83,67,98,90], and in contrast to [157,158,160,161,159], the proposed method can handle various factors that are unknown in reality, such as local load conditions and interactions with other units. This is achieved by treating these factors as unknown inputs while still estimating the states of all neighboring units.

4. In contrast to [49, 89, 83, 162, 98, 89, 90], which suffer from limitations such as the number of units under attack, the type of attack, or topology dependency, the proposed method has been tested under various types of cyber-attacks, including constant, time-varying, and unbounded FDIAs, as well as DoS attacks.

5. Unlike the methods discussed in [67,78,163], which experience high computation and execution times, the proposed method requires low computing time, making it conducive to real-time implementation.

6. Unlike the methods discussed in [2, 160, 98], the proposed method can detect cyber-attacks across all communication channels between units.

Table 2.4 . A brief review of the resilient control system design approaches

No	Study	Year	Attack type	Method	Advantages	Disadvantages
1	Sahoo et al. [164]	2020	MITM	Multilayer event-driven detection based on diverging factor	Locate the compromised link(s); Good robustness against MITM	Vulnerable to model uncertainties
2	Chen et al. [165]	2022	DoS	Resilient distributed control (PI & average consensus)	applicable against line impedance & CPL	Resiliency drops against large time-delays.
3	Zhou et al. [21]	2020	FDIA on three channels	Resilient signal-based controller	Considering attacks in various channels, Resilient against time-varying attacks	Medium computation load; Dependent on cyber graph connectivity
4	Liu et al. [32]	2021	FDI & DoS	Resilient controller (combined error with a pinning gain)	Observer with adaptive gains	Ignoring control constraint, Not robust to time delays & disturbances
5	Bidram et al. [144]	2019	Bounded FDIAs	Weighted Mean Subsequence Reduced algorithm	Improve the resiliency with time-varying communication Low processing load.	Computation burden; Attack number dependence
6	Sahoo et al. [81]	2020	Bounded FDIAs	Adaptive event-driven discord element algorithm	Simple design; resilience to PnP and single point of failure Low communication cost	—
7	Zuo et al. [20]	2020	Unbounded FDIAs	Fully distributed controller with virtual MAS	Unbounded attacks on various channels Not require any global information	High computation load
8	Li et al. [80]	2021	FDIA	Adaptive resilient secondary controller	Robustness to FDIAs; Attack's bound does not need to be known;	Vulnerable to other attacks time-delays
9	Zhao et al. [149]	2021	FDIA to actuators/sensors	Composite resilient controller (terminal SMO with adaptive gains)	Considering attacks on actuators and sensors, Low computation cost; Simple implementation	Exact model is required.
10	Song et al. [166]	2022	DoS attack	Adaptive resilient control (fractional-order backstepping)	Considering input delays and unknown sensor deception attacks;	High sensitivity to other attacks

2.4 Summary

The growing importance of enhancing the security of ac/dc MGs against various types of cyber-attacks has gained significant attention in recent years. This chapter provides a comprehensive review of recent advancements in this field, offering insights into the historical, current, and future developments. To begin, common cyber-attacks such as DoS, FDI, replay, and covert attacks are examined. Next, the chapter reviews existing schemes for cyber-attack detection, categorized into two main approaches: (a) attack detection and mitigation and (b) resilient control system design. In the first approach, existing methods for cyber-attack detection, including signal-based, model-based, and data-based schemes, are analyzed. The second approach focuses on resilient control system design, which ensures the robustness and resilience of MGs against cyber-attacks.

Chapter 3

Cyberattack Reconstruction and Mitigation with a Distributed Sliding Mode-based Unknown Input Observer for DC Microgrids

According to the reviewed literature, attack detection and mitigation of dc MGs is one of the crucial and hot topics that have recently been investigated with various approaches. In this regard, developing detection techniques that can deal with unknown inputs is an approach that many scholars have suggested. This chapter discusses developing an effective unknown input observer-based schemes for attack detection in the communication channels. In this regard, sliding mode-based UIO has been developed. After attack detection, we will use a method to mitigate destructive FDIA impacts. By doing so, safe operation for dc MGs in the presence of cyber-attack will be preserved.

This chapter contributes to the cybersecurity of dc MGs by making them robust and resistant to cyber threats. The present work has remedied the existing drawback in the literature by developing a novel distributed SM-based UIO to detect and mitigate the destructive effects of FDIAs in the communication links by cleaning the compromised signals. It also proposes an estimation of cyber-attacks based on the developed bank of observers. This chapter introduces a technique to estimate the states of neighboring DGs which is useful for remedy actions. The main contributions of this section of the chapter are as follows:

1. A new bank of SMO-based UIO is developed for cyber-attack reconstruction for coupled power and information networks in a dc MG by estimating the states in the neighbor DGs without the requirement of accessing to all inputs of other neighboring units.

2. A unified cyber-attack detection/mitigation scheme has been developed for dc MGs with vulnerable information networks, making them resilient and secure against FDIAs. The performance of this scheme has been evaluated against various types of cyber-attacks, including constant, time-varying FDIAs, and a type of DoS attack, through online detection and remedial actions

in the control center.

3. A technique is proposed to estimate cyber-attacks in communication channels with low computational complexity, which is designed for operation and control purpose in dc MGs.

3.1 Problem formulation: DC microgrid modeling

In this section, a continuous-time dynamic model of a dc MG, depicted in Fig. 3.1, is derived. Each DG unit has been modeled with a dc voltage source, dc-dc converter, LC filter, and local resistive loads. Moreover, it is assumed that power lines connecting each DG to its neighboring ones are all resistive.

Remark 3.1. *Since neighboring DGs communicate through current channels in the secondary control system, FDIAs are applied to this communication channel.*

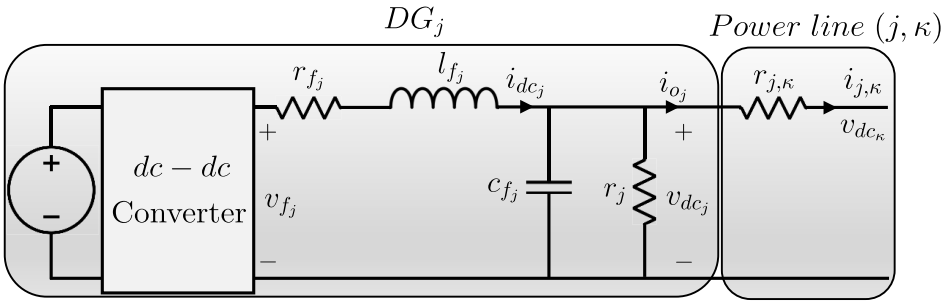


Figure 3.1 . Electrical scheme of a j-th DG and a resistive power line connecting the j-th DG to a k-th DG.

By assuming continuous mode and using the Kirchhoff's current and voltage laws, the mathematical model of the j-th DG can be derived as follows:

$$\begin{aligned} \dot{v}_{dc_j} &= \frac{1}{c_{f_j}}(i_{dc_j} - \sum_{\kappa \in \mathcal{N}_j} i_{j,\kappa} - \frac{1}{r_j} v_{dc_j}), \\ \dot{i}_{dc_j} &= \frac{1}{l_{f_j}}(v_{f_j} - r_{f_j} i_{dc_j} - v_{dc_j}). \end{aligned} \tag{3.1}$$

Here, v_{dc_j} and i_{dc_j} are the measurable load voltage and generated current. Therefore, $y_j = [v_{dc_j}\ i_{dc_j}]^T$ represents the output vector for the j-th DG. In (3.1), r_j, c_{f_j}, l_{f_j}, and r_{f_j} are the local

resistive load, shunt capacitor, filter inductance, and resistance, respectively; v_{f_j} is the j-th converter output voltage; $i_{j,k}$ denotes the line current between two neighboring DGs, calculated as $i_{j,k} = \frac{v_{dc_j} - v_{dc_k}}{r_{j,k}}$, where $r_{j,k}$ denotes the power line resistance. Moreover, the whole dc MG is modeled with an undirected communication graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ without self-loops, where the nodes in the set of $\mathcal{V}$ denote the DGs and the edges in the set of $\mathcal{E}$ represent the resistive power lines that connect the DGs. In addition, $\mathcal{N}_j$ denotes a subset of $\mathcal{E}$ which denotes the incident power lines connecting DG_j to its neighboring units. The considered graph topology can be represented with the following index matrix.

$$g_{j,\kappa} = \begin{cases} +1 & \mathrm{DG}_j \text{ connects to positive end of } \mathrm{DG}_\kappa, \\ 0 & \text{No connection}, \\ -1 & \mathrm{DG}_j \text{ connects to negative end of } \mathrm{DG}_\kappa. \end{cases} \tag{3.2}$$

To develop the SM-based UIO for attack detection, the dynamic equations of the dc MG are represented in the state-space as follows:

$$\begin{aligned} \dot{x}_j(t) &= A_j x_j(t) + B_j u_j(t), \\ y_j(t) &= C_j x_j(t), \end{aligned} \tag{3.3}$$

where $x_j(t) = [v_{dc_j} \;\; i_{dc_j}]^T \in \mathbb{R}^n$ and $y_j(t) \in \mathbb{R}^p$ denote the system state and output, with the dimensions of n and p, respectively. In this equation, $A_j \in \mathbb{R}^{n\times n}$, $B_j \in \mathbb{R}^{n\times m}$, and $C_j \in \mathbb{R}^{p\times n}$ represent the system, the input, and the output, which are considered to be known with some uncertainty. Cyber-attacks are applied to the sensor channels, and it is generally formulated as follows:

$$\tilde{y}_j(t) = y_j(t) + D_j a_j(t), \tag{3.4}$$

where $\tilde{y}_j(t)$ is the disrupted output signals and $D_j \in \mathbb{R}^{p\times 1}$ denotes the attack matrices. In addition, $a_j(t) \in \mathbb{R}$ is the FDIA signals to the sensors, where it targets the integrity of data by altering the communicated signals through injecting false data. This kind of attack is defined as follows:

$$a_j(t) = \begin{cases} 0 & \text{for } t \notin \tau_{a_j} \\ \lambda_j \mathcal{F}_j(.) & \text{for } t \in \tau_{a_j} \end{cases}, \tag{3.5}$$

where τ_a is the attack time period and λ is an attack parameter. In addition, $\mathcal{F}(.)$ can be either a time-/state-dependent function or completely independent. The following assumption is made to develop the proposed SM-based attack detection system.

Assumption 3.1. *It is assumed that some inputs are unknown. In this regard, assuming m as the dimension of the input vector, it is partitioned to m_1 and m_2 components, where the first m_1 components of u_j are known and transmitted through secure channels, and the m_2 components of u_j are unknown.*

According to *Assumption* 3.1, the input matrix can be partitioned into known and unknown inputs as $B_j = [B_{j,1}\ B_{j,2}]$, where $B_{j,1} \in \mathbb{R}^{n\times m_1}$ and $B_{j,2} \in \mathbb{R}^{n\times m_2}$, respectively. As a result, the input signal can be represented as follows:

$$u_j = \begin{bmatrix} u_{j,1} \\ u_{j,2} \end{bmatrix}. \tag{3.6}$$

Now, (3.3) can be described as:

$$\begin{aligned} \dot{x}_j(t) &= A_j x_j(t) + B_{j,1}u_{j,1}(t) + B_{j,2}u_{j,2}(t), \\ \tilde{y}_j(t) &= C_j x_j(t) + D_j a_j(t). \end{aligned} \tag{3.7}$$

To detect attacks on the system described in (3.7), an SM-based UIO is required for each neighboring DG_j. To this end, a bank of observers in each unit is developed to detect attacks in other units and secure the safe operation of an MG in the presence of cyber-attacks. The *Remark* 3.2 is made regarding the information unavailable from the neighboring units to facilitate the cyberattack-resilient control and operation method design and mimic the real-world complexity and industry challenges.

Remark 3.2. *It is assumed that the load conditions and the coupling effects of each DG are unknown to their neighbors [e.g., assume that DG j and k are neighbors; the $SMO_{k,j}$ (the observer located in DG j to estimate the states of DG k) considers $u_{k,2}(t) = \sum_{i\in\mathcal{N}_k} \frac{v_{dc_i}}{r_{i,k}} - \frac{v_{dc_k}}{r_k}$ as unknown input]. On the other hand, the output voltage of each converter (i.e., $u_{k,1}(t) = v_{f_k}$) is considered as a known input for the neighboring units.*

Remark 3.3. *Without loss of generality, $B_{j,2}$ is a full column rank matrix [88]. Even if it is not full column rank, then the rank-decomposition can be applied as $B_{j,2} = B^I_{j,2}B^{II}_{j,2}$, where $B^I_{j,2}$ is a full column rank matrix. Thus, we have:*

$$B_{j,2}u_{j,2}(t) = B^I_{j,2}B^{II}_{j,2}u_{j,2}(t) = \bar{B}_{j,2}\bar{u}_{j,2}(t), \tag{3.8}$$

where $\bar{B}_{j,2} = B^I_{j,2} \in \mathbb{R}^{n\times m_2}$ *is a full column rank matrix, and* $\bar{u}_{j,2}(t) = B^{II}_{j,2}u_{j,2}(t) \in \mathbb{R}^{m_2}$ *can be considered as a new unknown input.*

Thus, the matrices for the considered dc MG are defined as follows:

$$A_j = \begin{bmatrix} -\sum_{k\in\mathcal{N}_j} \frac{1}{c_{f_j} r_{j,k}} & \frac{1}{c_{f_j}} \\ -\frac{1}{l_{f_j}} & -\frac{r_{f_j}}{l_{f_j}} \end{bmatrix}, B_{j,1} = \begin{bmatrix} 0 \\ \frac{1}{l_{f_j}} \end{bmatrix}, B_{j,2} = \begin{bmatrix} \frac{1}{c_{f_j}} \\ 0 \end{bmatrix}, C_j = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, D_j = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{3.9}$$

In the next section, a bank of SM-based UIOs is designed for each DG to provide safe operation of the MG by detecting cyberattacks and mitigating their destructive impacts through an advanced cyberattack-resilient control and operation framework.

3.2 Distributed sliding mode unknown input observer

This section discusses a bank of SM-based UIO to estimate the states of all neighboring units for attack reconstruction purposes. With this bank of SM-based observers, which should be provided for all DGs, the states of all neighboring DGs can be estimated. By doing so, any probable cyber-attacks in the communication channels can be reconstructed in finite time by comparing the estimated states values with the measured ones. Figure 3.2 shows the structure of the proposed technique. According to *Remark* 3.1, the polluted signal is represented as $\tilde{i}_{dc_j} = i_{dc_j} + a_j$. From a mathematical point of view, cyber-attacks applied to the current channels can be detected with this method as follows:

$$\hat{a}_j = \tilde{i}_{dc_j} - \hat{i}_j, \tag{3.10}$$

where $\hat{a}_j(t)$ and $\hat{i}_j(t)$ denote the detected attack signal and the estimated current values, respectively. According to (3.10), it is evident that $\|\hat{i}_{dc_j} - i_{dc_j}\| \to 0$ implies $\|a_j - \hat{a}_j\| \to 0$. Thus, the problem of attack detection is transformed to an observer design problem.

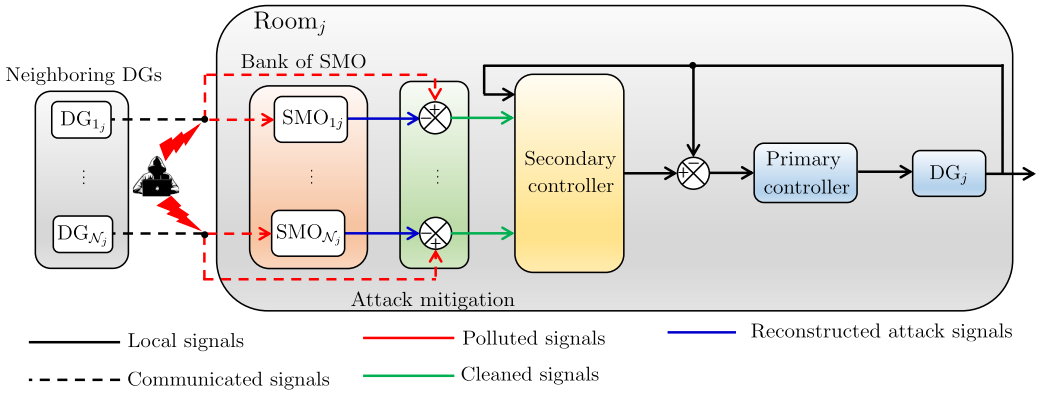


Figure 3.2 . General scheme of the proposed FDIA detection and mitigation strategy.

To reconstruct cyber-attacks with the proposed scheme, the dynamic model of each DG is augmented in the state-space form, as follows:

$$\begin{aligned} \dot{z}_j(t) &= \bar{A}_j z_j(t) + \bar{B}_{j,1} u_{j,1}(t) + \bar{B}_{j,2} u_{j,2}(t), \\ \tilde{y}_j(t) &= \bar{C}_j z_j(t), \end{aligned} \tag{3.11}$$

where $z_j = [x_j^T \ a_j]^T$ denotes the augmented state. Here, $\bar{A}_j \in \mathbb{R}^{(n+1)\times(n+1)}$, $\bar{B}_{j,1} \in \mathbb{R}^{(n+1)\times m_1}$, $\bar{B}_{j,2} \in \mathbb{R}^{(n+1)\times m_2}$, and $\bar{C}_j \in \mathbb{R}^{p\times(n+1)}$ denote the augmented matrices and vectors with appropriate size, where it is assumed that $(n+1) > m_2$. The augmented matrices are defined as follows:

$$\bar{A}_j = \left[\begin{array}{c|c} A_j & \mathbf{0}_{2\times 1} \\ \hline \mathbf{0}_{1\times 2} & 0 \end{array}\right], \bar{B}_{j,1} = \left[\begin{array}{c} B_{j,1} \\ \hline 0 \end{array}\right], \bar{B}_{j,2} = \left[\begin{array}{c} B_{j,2} \\ \hline 0 \end{array}\right], \bar{C}_j = \left[\begin{array}{c|c} C & D \end{array}\right]. \tag{3.12}$$

In the next section, the proposed SMO-based UIO is developed to reconstruct attack signals in the communication channels.

3.2.1 Proposed SMO-based attack reconstruction

According to *Remark* 3.1, the attacked signal is represented as $\tilde{i}_{dc_j} = i_{dc_j} + a_j$. Thus, the output signal can be expressed as $\tilde{y}_j(t) = [v_{dc_j} \ \tilde{i}_{dc_j}]$. Before developing the proposed full-order SM-based UIO to detect the applied attacks and estimate the states of neighboring DGs, it is necessary to express the following assumption regarding the boundedness of unknown inputs.

Assumption 3.2. *It is assumed that the unknown inputs [i.e., $u_{j,2}(t)$] are bounded. In other words, for all $t \geq 0$, we have*

$$|u_{j,2}(t)| \leq \rho_j,$$

where ρ_j denotes the upper bound of unknown inputs.

Let $\hat{z}_j(t)$ be an estimate of $z_j(t)$ and $\mathcal{E} = \hat{z}_j(t) - z_j(t)$ denotes the estimation error. An observer gain $\bar{L}_j \in \mathbb{R}^{(n+1)\times p}$ exists provided that the pair $\left(\bar{A}_j, \bar{C}_j\right)$ is observable. If it holds, the matrix $\left(\bar{A}_j - \bar{L}_j\bar{C}_j\right)$ will be Hurwitz. As a result, from the Lyapunov stability point of view, for any $Q_j \in \mathbb{R}^{(n+1)\times(n+1)} > 0$, there exists a unique $P_j \in \mathbb{R}^{(n+1)\times(n+1)} > 0$ so that

$$(\bar{A}_j - L_j\bar{C}_j)^T P_j + P_j(\bar{A}_j - L_j\bar{C}_j) = -Q_j. \tag{3.13}$$

It will be shown that the proposed observer is realizable provided that for some $F_j \in \mathbb{R}^{m_2\times p}$, we have

$$F_j\bar{C}_j = \bar{B}_{j,2}^T P_j. \tag{3.14}$$

Thus, by defining the sliding surface as $\mathcal{S}_j = F_j\bar{C}\mathcal{E} = \mathbf{0}$, the observer in (3.15) can asymptotically estimate the state $z_j(t)$ of the dynamic system described in (3.11).

$$\dot{\hat{z}}_j = \bar{A}_j\hat{z}_j + \bar{B}_{j,1}u_{j,1} + \bar{L}_j(\tilde{y}_j - \hat{y}_j) + \bar{B}_{j,2}\mathcal{H}_j(\tilde{y}_j - \hat{y}_j, \eta_j), \tag{3.15}$$

where $\hat{y}_j(t) = \bar{C}_j\hat{z}_j(t)$ is the estimated output vector. Moreover, $\mathcal{H}_j(\tilde{y}_j - \hat{y}_j, \eta)$ denotes a vector function that can be described as follows:

$$\mathcal{H}_j(\tilde{y}_j - \hat{y}_j, \eta_j) = \begin{cases} \eta_j \frac{F_j(\tilde{y}_j - \hat{y}_j)}{\|F_j(\tilde{y}_j - \hat{y}_j)\|_2} & \text{for } \; F_j(\tilde{y}_j - \hat{y}_j) \neq 0, \\ 0 & \text{for } \; F_j(\tilde{y}_j - \hat{y}_j) = 0. \end{cases} \tag{3.16}$$

It is worth noting that for $\eta_j \geq \rho_j$, the estimation error converges to zero asymptotically. Notes that η_j must exceed the maximum uncertainty bound. Choosing a larger η_j yields more aggressive switching and thus increased chattering, whereas a smaller η_j reduces chattering but may compromise robustness if it sits too close to the uncertainty bound. To prove this statement by Lyapunov stability theory, we express the error signal by using (3.11) and (3.15), as follows:

$$\dot{\mathcal{E}}_j = (\bar{A}_j - \bar{L}_j\bar{C}_j)\mathcal{E}_j + \bar{B}_{j,2}u_2 - \bar{B}_{j,2}\mathcal{H}_j(\tilde{y}_j - \hat{y}_j, \eta_j). \tag{3.17}$$

Thanks to (3.16) and the parameter selection such that $\eta_j \geq \rho_j$, it can be concluded that along the convergence of the sliding surface to zero, we have

$$\lim_{t\to\infty} \mathcal{E}_j(t) = 0. \tag{3.18}$$

In what follows, the subscript (j) is omitted to simplify the representation of the equations, where necessary explanations are given wherever needed.

Theorem 3.1. *Under Assumption 3.2, if we apply the SMO given by* (3.13) - (3.16) *to system* (3.11)*, then the state estimation error dynamics given by* (3.17) *is globally asymptotically stable, that is, for any initial conditions, we have* $\lim_{t\to\infty} s(t) = 0$*, which results in* $\mathcal{E}$ *going to zero.*

Proof: The dynamic representation of the dc MG and the proposed SMO are expressed in (3.11) and (3.15). Recall that $\tilde{y}(t) = [v_{dc},\ i_{dc} + a(t)]$ and $\hat{y}(t) = \bar{C}\hat{z}(t)$, and $\hat{z} = [\hat{x}^T\ \hat{a}]^T$.

As already mentioned, the sliding surface is $\mathcal{S} = \{t \in R^+ : s(t) = 0 \mid s(t) = F\bar{C}\mathcal{E}\}$, where $\mathcal{E} = \begin{bmatrix} e \\ e_a \end{bmatrix}$, $e = x - \hat{x}$ and $e_a = a - \hat{a}$. The augmented error system can be represented as:

$$\dot{\mathcal{E}} = \underbrace{(\bar{A} - \bar{L}\bar{C})}_{\mathcal{A}}\mathcal{E} + \bar{B}_2 u_2 - \bar{B}_2\eta\frac{F\bar{C}\mathcal{E}}{\|F\bar{C}\mathcal{E}\|}. \tag{3.19}$$

Thanks to the fact that $u_2(t)$ is bounded, $\mathcal{A}$ is Hurwitz, and $F\bar{C}\mathcal{E}$ is bounded, we can consider the upper bound of $\mathcal{E}$ to be limited by k. In the sequence, the stability proof of the proposed observer is provided. For this aim, the time derivative of sliding surface is calculated as:

$$\dot{s} = F\bar{C}\dot{\mathcal{E}} = F\bar{C}(\mathcal{A}\mathcal{E} + \bar{B}_2 u_2 - \bar{B}_2\eta\frac{F\bar{C}\mathcal{E}}{\|F\bar{C}\mathcal{E}\|}). \tag{3.20}$$

To prove the stability of the proposed observer, the candidate Lyapunov is chosen as $V(s) = \frac{1}{2}s^T s$. Thus, we have:

$$\begin{aligned} \dot{V} = s^T\dot{s} &= s^T(F\bar{C}(\mathcal{A}\mathcal{E} + \bar{B}_2 u_2 - \bar{B}_2\eta\frac{F\bar{C}\mathcal{E}}{\|F\bar{C}\mathcal{E}\|})), \\ &= s^T F\bar{C}\mathcal{A}\mathcal{E} + s^T F\bar{C}\bar{B}_2 u_2 - s^T F\bar{C}\bar{B}_2\eta\frac{F\bar{C}\mathcal{E}}{\|F\bar{C}\mathcal{E}\|}. \end{aligned} \tag{3.21}$$

Thanks to $F\bar{C} = \bar{B}_2^T P$, we have:

$$\begin{aligned} \dot{V} &\leq \|F\bar{C}\mathcal{A}\|\|\mathcal{E}\|\|s\| + s^T(\bar{B}_2^T P\bar{B}_2)u_2 - \eta s^T(\bar{B}_2^T P\bar{B}_2)\frac{s}{\|s\|} \\ &\leq k\|F\bar{C}\mathcal{A}\|\|s\| + \lambda_{max}(\bar{B}_2^T P\bar{B}_2)\|u_2\|\|s\| \\ &-\eta\lambda_{min}(\bar{B}_2^T P\bar{B}_2)\|s\| = -(\eta - \bar{\eta})\lambda_{min}(\bar{B}_2^T P\bar{B}_2)\|s\|, \end{aligned} \tag{3.22}$$

where

$$\bar{\eta} = \frac{k\|F\bar{C}\mathcal{A}\| + \rho\lambda_{max}(\bar{B}^T P\bar{B})}{\lambda_{min}(\bar{B}^T P\bar{B})},$$

where $\lambda_{min}(\bar{B}^T P \bar{B}) > 0$ as $\bar{B}$ is of full column rank. Thus, if we choose η such that $\eta \geq \bar{\eta} + \frac{\gamma}{\lambda_{min}(\bar{B}^T P \bar{B})}$, where γ is a small positive constant, then $s^T \dot{s} \leq -\gamma \|s\|$, which implies that the surface $s(t) = F\bar{C}\mathcal{E}$ is invariant. Then we can show that the sliding surface is reached in a finite time [167]. ■

The term "robustness" in the context of MGs refers to the system's ability to maintain resilient performance despite cyberattacks. To achieve this, the proposed UIO-based schemes are designed to estimate both the system states and the attack signals present in communication channels, even amidst parameter uncertainties and unknown inputs. Once these signals are accurately estimated and filtered, they are fed into the control system, where a simple PI controller ensures that the desired objectives of the MG are achieved. This approach enhances the MG's resilience against cyber threats by effectively detecting and mitigating potential disruptions. In addition to the mathematical proof of the robustness of the proposed scheme, several simulation studies have demonstrated its robust performance.

The following discusses the necessary and sufficient conditions for the observer's existence and how the essential ingredients to establish this SMO-based detector should be determined.

Condition 3.1. $\text{rank}(\bar{B}_2) = \text{rank}(\bar{C}\bar{B}_2) = \zeta$, *where* $\zeta < p$. *This implies that this method is applicable when the number of outputs is greater than the number of unknown inputs.*

Now, the following lemma is required to proceed with the proposed SMO design to detect cyber-attacks for systems with unknown inputs [168].

Lemma 3.1. *Let's assume that Condition 3.1 holds true. Then, for the triple* $(\bar{A},\ \bar{B}_2,\ \bar{C})$, *there exist matrices* $T \in \mathbb{R}^{(n+1)\times(n+1)}$ *and* $S \in \mathbb{R}^{p\times p}$ *such that [168]:*

$$\check{A} = T\bar{A}T^{-1} = \begin{bmatrix} \check{A}_{11} & \check{A}_{12} \\ \check{A}_{21} & \check{A}_{22} \end{bmatrix}, \check{B}_2 = T\bar{B}_2 = \begin{bmatrix} \check{B}_{2_1} \\ 0 \end{bmatrix}, \check{C} = S\bar{C}T^{-1} \ = \begin{bmatrix} I_\zeta & 0 \\ 0 & \check{C}_{22} \end{bmatrix}. \tag{3.23}$$

In the above equation, $\check{A}_{11} \in \mathbb{R}^{\zeta\times\zeta}$, $\check{A}_{12} \in \mathbb{R}^{\zeta\times(n+1-\zeta)}$, $\check{A}_{21} \in \mathbb{R}^{(n+1-\zeta)\times\zeta}$, $\check{A}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(n+1-\zeta)}$, $\check{B}_{2_1} \in \mathbb{R}^{\zeta\times m_2}$, *where* $\text{rank}(\check{B}_{2_1}) = \zeta$, *and* $\check{C}_{22} \in \mathbb{R}^{(p-\zeta)\times(n+1-\zeta)}$.

Proof. To prove this lemma, the Q-R decomposition is applied to $\bar{B}_2 \in \mathbb{R}^{(n+1)\times m_2}$, as follows:

$$\bar{B}_2 = Q_{\bar{B}_2} R_{\bar{B}_2}. \tag{3.24}$$

According to the features of the Q-R decomposition [168], $Q_{\bar{B}_2} \in \mathbb{R}^{(n+1)\times(n+1)}$ is a unitary matrix and $R_{\bar{B}_2} = \left[\tilde{B}_{2_1}^T,\ 0\right]^T \in \mathbb{R}^{(n+1)\times m_2}$ and $\tilde{B}_{2_1} \in \mathbb{R}^{\zeta\times m_2}$ is an upper triangular matrix with $\text{rank}(\tilde{B}_{2_1}) = \zeta$ [169].

To unify the notation, let $T_1 = Q_{\bar{B}_2}^{-1}$. Now, by multiplying matrix $\bar{C}$ by T_1^{-1}, it is partitioned as follows:

$$\bar{C}T_1^{-1} = \tilde{C} = \left[\begin{array}{cc} \tilde{C}_1 & \tilde{C}_2 \end{array}\right], \tag{3.25}$$

where $\tilde{C}_1 \in \mathbb{R}^{p\times\zeta}$ and $\tilde{C}_2 \in \mathbb{R}^{p\times(n+1-\zeta)}$. With respect to (3.24) and (3.25), $\bar{C}\bar{B}_2$ can be obtained as

$$\bar{C}\bar{B}_2 = (\bar{C}T_1^{-1})(T_1\bar{B}_2) = \tilde{C}_1\tilde{B}_{2_1}. \tag{3.26}$$

Now, we apply the Q-R decomposition to matrix $\tilde{C}_1$, so we have

$$\tilde{C}_1 = Q_{\tilde{C}_1}R_{\tilde{C}_1}. \tag{3.27}$$

In the above equation, $Q_{\tilde{C}_1} \in \mathbb{R}^{p\times p}$ is a unitary matrix and $R_{\tilde{C}_1} = \left[\tilde{C}_{11}^T,\ 0\right]^T \in \mathbb{R}^{p\times\zeta}$ and $\tilde{C}_{11} \in \mathbb{R}^{\zeta\times\zeta}$ is an upper triangular matrix with $\text{rank}(\tilde{C}_{11}) = \zeta$ and invertible [169]. Now, by pre-multiplying both sides of (3.25) by $Q_{\tilde{C}_1}^{-1}$ and using (3.27), we obtain:

$$Q_{\tilde{C}_1}^{-1}\tilde{C} = \left[\begin{array}{cc} \tilde{C}_{11} & \tilde{C}_{12} \\ 0 & \tilde{C}_{22} \end{array}\right]. \tag{3.28}$$

To unify the notation, let $S = Q_{\tilde{C}_1}^{-1}$. To achieve the last relationship of (3.23), T_2^{-1} is defined as follows:

$$T_2^{-1} = \left[\begin{array}{cc} \tilde{C}_{11}^{-1} & -\tilde{C}_{11}^{-1}\tilde{C}_{12} \\ 0 & I_{n-\zeta} \end{array}\right]. \tag{3.29}$$

By using (3.28) and (3.29), we obtain

$$\check{C} = S\tilde{C}T_2^{-1} = S\bar{C}T_1^{-1}T_2^{-1} = \left[\begin{array}{cc} I_\zeta & 0 \\ 0 & \tilde{C}_{22} \end{array}\right]. \tag{3.30}$$

To unify the notation, let $T = T_2T_1$. Also, $\check{B}_2 = T_2R_{\bar{B}_2}$. ■

Condition 3.2. *The pair* $(\check{A}_{22},\ \check{C}_{22})$ *should be detectable.*

Lemma 3.2. *Let's assume that Condition 3.1 holds true. Then, Condition 3.2 is satisfied if and only if, for all s such that $Re(s) \geq 0$, we have*

$$\operatorname{rank} \underbrace{\begin{bmatrix} sI_{(n+1)} - \check{A} & \check{B}_2 \\ \check{C} & 0 \end{bmatrix}}_{\Lambda} = n + 1 + \zeta. \tag{3.31}$$

Proof. To prove this lemma, we use the Popov-Belevitch-Hautus test [81]. By substituting $\check{A}$, $\check{B}_2$, and $\check{C}$ from (3.23) in (3.31), we have

$$\operatorname{rank} \begin{bmatrix} sI_{\zeta} - \check{A}_{11} & -\check{A}_{12} & \check{B}_{2_1} \\ -\check{A}_{21} & sI_{(n+1-\zeta)} - \check{A}_{22} & 0 \\ I_{\zeta} & 0 & 0 \\ 0 & \check{C}_{22} & 0 \end{bmatrix} = \operatorname{rank} \begin{bmatrix} -\check{A}_{12} & \check{B}_{2_1} \\ sI_{(n+1-\zeta)} - \check{A}_{22} & 0 \\ \check{C}_{22} & 0 \end{bmatrix} + \zeta. \tag{3.32}$$

According to *Condition* 3.1 and its proof, $\check{B}_{2_1} \in \mathbb{R}^{\zeta \times m_2}$, and $\operatorname{rank}(\check{B}_{2_1}) = \zeta$; thus:

$$\operatorname{rank}(\Lambda) = \operatorname{rank} \begin{bmatrix} sI_{(n+1-\zeta)} - \check{A}_{22} \\ \check{C}_{22} \end{bmatrix} + 2\zeta. \tag{3.33}$$

Equation (3.33) clearly shows that the pair $(\check{A}_{22},\ \check{C}_{22})$ is detectable provided that (3.31) is fulfilled.

■

In the following, *Theorem* 3.2 is provided to construct matrices $\bar{L} \in \mathbb{R}^{(n+1)\times p}$, $P \in \mathbb{R}^{(n+1)\times(n+1)}$, and $F \in \mathbb{R}^{m_2 \times p}$, which are necessary to design the proposed SM-based UIO for state estimation and attack reconstruction. A layout of the proposed SM-based UIO is illustrated in Fig. 3.3. In this figure, the green block represents the dynamic of the system, represented in augmented form, including both known and unknown inputs. In yellow block, the proposed observer-based attack detection is shown. For this purpose, a proper sliding surface is selected as $s_j(t) = F_j \bar{C}_j \mathcal{E}_j$, where F_j is obtained with the appropriate transformation matrices (i.e., T and S). Then, the required observer gain matrices [i.e., $\bar{L}_j$ and $\mathcal{H}_j(\tilde{y}_j - \hat{y}_j, \eta_j)$] are used to design the proposed observer for state estimation. Then, the constructed attack signals are used to mitigate their destructive effects on the system.

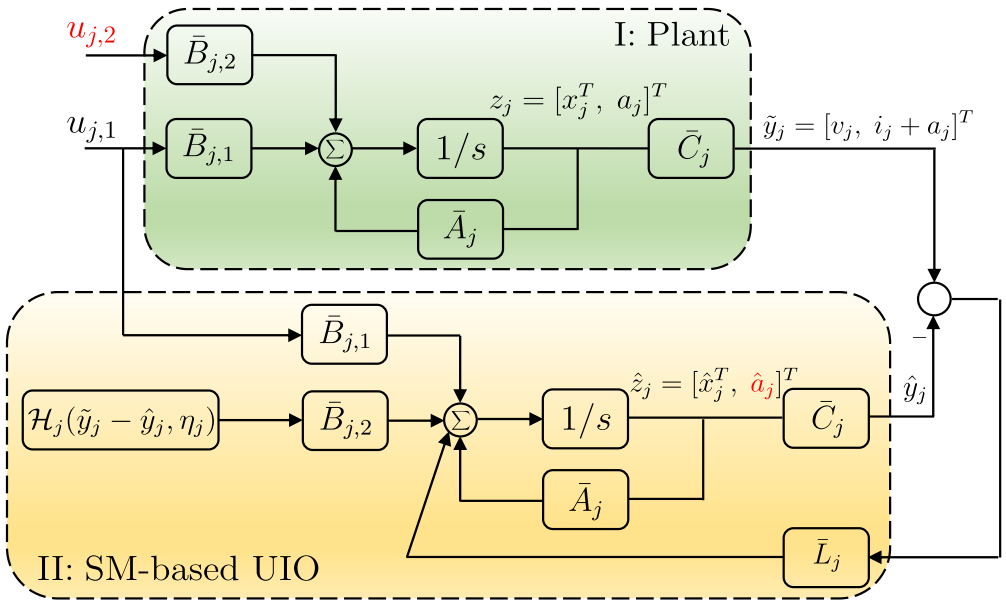


Figure 3.3 . The structure of the proposed SM-based UIO

Theorem 3.2. *Conditions 3.1 and 3.2 hold true if and only if, for all s such that $Re(s) \geq 0$, a triple of matrices $L \in \mathbb{R}^{(n+1)\times p}$, $P \in \mathbb{R}^{(n+1)\times(n+1)}$, and $F \in \mathbb{R}^{m_2 \times p}$ exit such that*

$$(\bar{A} - L\bar{C})^T P + P(\bar{A} - L\bar{C}) < 0, \tag{3.34}$$

and

$$F\bar{C} = \bar{B}_2^T P, \tag{3.35}$$

where P is a positive definite matrix.

Proof. According to *Lemma* 3.2, if *Condition* 3.1 is satisfied, then there exists non-singular matrices T and S so that (3.23) is established. In addition, *Condition* 3.2 is equivalent to the existence of a matrix $\check{L}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(p-\zeta)}$ so that the matrix $(\check{A}_{22} - \check{L}_{22}\check{C}_{22})$ is Hurwitz. Therefore, from the Lyapunov stability point of view, it can be shown that for any symmetric positive definite $\check{Q}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(n+1-\zeta)}$, there exists a symmetric positive definite $\check{P}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(n+1-\zeta)}$ satisfying the following Lyapunov matrix equation.

$$\left(\check{A}_{22} - \check{L}_{22}\check{C}_{22}\right)^T \check{P}_{22} + \check{P}_{22}\left(\check{A}_{22} - \check{L}_{22}\check{C}_{22}\right) = -\check{Q}_{22}. \tag{3.36}$$

Note that the system will exhibit different responses depending on the weight matrix $\check{Q}_{22}$. As a result, this matrix parameter gives designers a broad flexibility to consider various dynamic responses.

We now show that the detectability of the pair $(\check{A}_{22}, \check{C}_{22})$ implies the existence of matrices P, $\bar{L}$ and F satisfying (3.34) and (3.35). For this purpose, let (see [167])

$$\check{P} = T^{-T} P T^{-1}, \quad \check{L} = T\bar{L}S^{-1}, \quad \check{F} = FS^{-1}. \tag{3.37}$$

In the above equation, let (see [167])

$$\check{L} = \begin{bmatrix} \upsilon I_\zeta & 0 \\ 0 & \check{L}_{22} \end{bmatrix}, \check{P} = \begin{bmatrix} I_\zeta & 0 \\ 0 & \check{P}_{22} \end{bmatrix}, \check{Q} = \begin{bmatrix} \check{Q}_{11} & \check{Q}_{12} \\ \check{Q}_{12}^T & \check{Q}_{22} \end{bmatrix}, \tag{3.38}$$

where $\upsilon > 0$ is a design parameter that will be determined later. Noted that selecting a very large value for υ leads to faster error convergence; however, it may also introduce numerical sensitivity. Conversely, choosing a very small υ may fail to satisfy the Lyapunov inequality, potentially resulting in instability.. Now, by substituting (3.23) and (3.38) into the Lyapunov matrix equation (3.13), the following three relationships can be satisfied, which are required for stability purposes.

$$\begin{aligned} \check{Q}_{11} &= -\left(\check{A}_{11} + \check{A}_{11}^T - 2\upsilon I_\zeta\right), \\ \check{Q}_{12} &= -\left(\check{A}_{12} + \check{A}_{21}^T \check{P}_{22}\right), \\ \check{Q}_{22} &= -\left((\check{A}_{22} - \check{L}_{22}\check{C}_{22})^T \check{P}_{22} + \check{P}_{22}(\check{A}_{22} - \check{L}_{22}\check{C}_{22})\right). \end{aligned} \tag{3.39}$$

As mentioned above, $\check{Q}_{22}$ is a positive definite matrix. Hence, according to the Schur complement [170], $\check{Q} > 0$, if and only if

$$\check{Q}_{11} > \check{Q}_{12}\check{Q}_{22}^{-1}\check{Q}_{12}^T. \tag{3.40}$$

It is required to determine the lower bound on the parameter υ such that the matrix $\check{Q}$ becomes positive definite. For this purpose, (3.39) is substituted into (3.40), and doing some algebraic calculations, we have that;

$$2\upsilon I_\zeta > \tilde{Q}, \tag{3.41}$$

where

$$\tilde{Q} = \check{A}_{11} + \check{A}_{11}^T + \left(\check{A}_{12} + \check{A}_{21}^T \check{P}_{22}\right) \check{Q}_{22}^{-1} \left(\check{A}_{12}^T + \check{P}_{22}\check{A}_{21}\right). \tag{3.42}$$

Therefore, we can conclude from (3.42) that $\check{Q}$ is positive definite if

$$\upsilon > \frac{1}{2}\lambda_{\max}(\tilde{Q}). \tag{3.43}$$

Finally, it follows that:

$$\check{F} = \begin{bmatrix} \check{B}_{2_1}^T & 0 \end{bmatrix}. \tag{3.44}$$

Now, thanks to the structure of $\check{B}_2$, $\check{C}$, and $\check{P}$, it is easy to see that (3.34) and (3.35) are fulfilled. Thus, the sufficiency conditions for the existence of the desired $\bar{L}$, P, and F matrices are guaranteed.

To highlight the necessity, we show that *Theorem* 3.2 implies that *Condition* 3.1 and *Condition* 3.2 hold. Since P is positive definite, then, it is easy to show that $\operatorname{rank}(\bar{B}_2^T P \bar{B}_2) = \operatorname{rank} \bar{B}_2$ [171]. Now, by post-multiplying both sides of (3.35) by $\bar{B}_2$, it follows that $\operatorname{rank}(\bar{B}_2^T P \bar{B}_2) = \operatorname{rank}(F\bar{C}\bar{B}_2) \leq \operatorname{rank}(\bar{C}\bar{B}_2) \leq \operatorname{rank}(\bar{B}_2)$. Thus, $\operatorname{rank}(\bar{C}\bar{B}_2) = \operatorname{rank}(\bar{B}_2)$.

According to *Lemma* 3.1, it was shown that if *Condition* 3.1 holds true, then there exist transformation matrices (i.e., T and S) such that (3.23) is established. Now, we show that if *Theorem* 3.1 holds true, then it follows that the pair $(\check{A}_{22},\ \check{C}_{22})$ is detectable. In other words, *Condition* 3.2 holds.

According to (3.37), $P = T^T \check{P} T$, $\bar{L} = T^{-1}\check{L}S$, and $F = \check{F}S$, where P is a symmetric matrix. Then, by *Theorem* 3.1, it implies that (3.34) and (3.35) hold. Let's consider that:

$$\check{P} = \begin{bmatrix} \check{P}_{11} & \check{P}_{12} \\ \check{P}_{21} & \check{P}_{22} \end{bmatrix}, \check{L} = \begin{bmatrix} \check{L}_{11} & \check{L}_{12} \\ \check{L}_{21} & \check{L}_{22} \end{bmatrix}, \check{F} = \begin{bmatrix} \check{F}_1 & \check{F}_2 \end{bmatrix}, \tag{3.45}$$

where $\check{P}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(n+1-\zeta)}$, $\check{L}_{22} \in \mathbb{R}^{(n+1-\zeta)\times(p-\zeta)}$, and $\check{F}_2 \in \mathbb{R}^{m_2\times(p-\zeta)}$. Now, by substituting (3.45) into (3.34) and (3.35), we obtain

$$\check{P}_{21}\left(\check{A}_{12} - \check{L}_{12}\check{C}_{22}\right) + \check{P}_{22}\left(\check{A}_{22} - \check{L}_{22}\check{C}_{22}\right) + \left(\check{A}_{12} - \check{L}_{12}\check{C}_{22}\right)^T \check{P}_{12} + \left(\check{A}_{22} - \check{L}_{22}\check{C}_{22}\right)^T \check{P}_{22} < 0. \tag{3.46}$$

In addition, from (3.35), we know that $\check{B}_{2_1}^T \check{P}_{12} = \check{F}_2\check{C}_{22}$, and $\check{B}_{2_1}\check{B}_{2_1}^T$ is invertible because $\check{B}_{2_1}$ has full row rank. Thus, we conclude that $\check{P}_{12} = (\check{B}_{2_1}\check{B}_{2_1}^T)^{-1}\check{B}_{2_1}\check{F}_2\check{C}_{22}$. Substituting it into (3.46) yields

$$\check{P}_{22}\left(\check{A}_{22} - \check{\bar{L}}_{22}\check{C}_{22}\right) + \left(\check{A}_{22} - \check{\bar{L}}_{22}\check{C}_{22}\right)^{\mathrm{T}} \check{P}_{22} < 0, \tag{3.47}$$

where

$$\check{\bar{L}}_{22} = \check{L}_{22} - \check{P}_{22}^{-1}\left(\check{A}_{12} - \check{L}_{12}\check{C}_{22}\right)^{\mathrm{T}}\left(\check{B}_2\check{B}_2^{\mathrm{T}}\right)^{-1}\check{B}_2\check{F}_2. \tag{3.48}$$

Since $\check{P}_{22}$ is symmetric and positive definite, (3.47) implies that $(\check{A}_{22} - \check{\bar{L}}_{22}\check{C}_{22})$ is Hurwitz, and as a result, the pair $(\check{A}_{22}, \check{C}_{22})$ is detectable. This completes the proof. ■

3.2.2 State-space Kalman filter design to estimate the local states

The effect of noise in the measurement is a factor that cannot be ignored. To address this issue, a KF observer is designed in each DG to clean the local measurement signals. For this aim, the dynamic equations of j-th DG are expressed as follows:

$$\begin{aligned} \dot{x}_j(t) &= A_{l_j} x_j(t) + B_{l_j} u_j(t) + G_{l_j} w_j(t), \\ y_j(t) &= C_{l_j} x_j(t) + n_j(t). \end{aligned} \tag{3.49}$$

Here, $A_{l_j} \in \mathbb{R}^{n\times n}$, $B_{l_j} \in \mathbb{R}^{n\times(\sigma_j+1)}$, $C_{l_j} \in \mathbb{R}^{p\times n}$, and $G_{l_j} \in \mathbb{R}^{n\times g}$, where $g \leq n$ and σ_j denotes the number of neighboring units of the j-th DG. Additionally, $w_j(t)$ and $n_j(t)$ are the process and measurement noises, which is assumed to be white noises with zero mean value (i.e., $E[w_j(t)] = E[n_j(t)] = 0$). The matrices in (3.49) are defined as follows:

$$A_{l_j} = \begin{bmatrix} -\frac{1}{c_{f_j} r_j} - \sum_{k\in\mathcal{N}_j} \frac{1}{c_{f_j} r_{j,k}} & \frac{1}{c_{f_j}} \\ -\frac{1}{l_{f_j}} & -\frac{r_{f_j}}{l_{f_j}} \end{bmatrix}, B_{l_j} = \begin{bmatrix} \mathrm{diag}[\frac{1}{c_{f_j} r_{j,k}}]_{k\in\mathcal{N}_j} & 0 \\ 0 & \frac{1}{l_{f_j}} \end{bmatrix}, C_{l_j} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3.50}$$

It is worth mentioning that $u_j(t) = \begin{bmatrix} [v_{dc_k}]_{k\in\mathcal{N}_j} & v_{t_j} \end{bmatrix}^T \in \mathbb{R}^{(N_j+1)}$, where v_{dc_k}, for $k \in \mathcal{N}_j$, is obtained from the SM-based unknown input observers and N_j denotes the number of neighbors. Now, by considering (3.49), the following KF observer is designed [88].

$$\begin{aligned} \dot{\hat{x}}_j(t) &= A_{L_j} \hat{x}_j(t) + B_{L_j} u_j(t) + K_{kf_j}(y_j - \hat{y}_j), \\ \hat{y}_j(t) &= C_{L_j} \hat{x}_j(t), \end{aligned} \tag{3.51}$$

where the KF gain, K_{kf_j}, can be obtained as

$$K_{kf_j} = P_{kf_j} C_{L_j}^T R_{kf_j}^{-1}. \tag{3.52}$$

In (3.52), P_{kf_j} is a positive definite matrix that can be achieved by solving the following Riccati equation:

$$P_{kf_j} A_{L_j}^T + A_{L_j} P_{kf_j} - P_{kf_j} C_{L_j}^T R_{kf_j}^{-1} C_{L_j} P_{kf_j} + Q_{kf_j} = 0, \tag{3.53}$$

where $Q_{kf_j} \geq 0$ and $R_{kf_j} > 0$ represent the measures of the noise level in the process and output sensors, respectively.

After cleaning the local signals from noises and detecting cyber-attacks with the proposed SM-based unknown input observers, we can mitigate the effects of FDIAs by cleaning the compromised signals.

3.2.3 Proposed observer implementation

This section discusses how this novel SM-based UIO can be implemented for an MG. First, the transformation in (3.23) is conducted. Then, matrices $\bar{L}$ and F must be constructed. For this purpose, $\check{L} = f(\upsilon, \check{L}_{22})$ should be calculated, where υ is obtained with (3.43) and $\check{L}_{22}$ is selected by the pole-placement approach so that the matrix $(\check{A}_{22} - \check{L}_{22}\check{C}_{22})$ is Hurwitz. Thanks to the applied transformation and regardless of the number of DGs, the order of each observer is two. To design the gain of the proposed observer (i.e., $\check{L}_{22}$), the standard second-order pole-placement approach can be used, note that the observer poles must be 5 to 10 times faster than the controller poles. The speed of each observer can be tuned with the damping ratio and frequency of that observer. After calculating $\check{L}$ and $\check{F}$, $\bar{L}$ and F can be obtained easily with (3.37). Finally, the proposed SM-based UIO can be designed by (3.15). It should be emphasized that before implementing this scheme, *Conditions* 3.1 and 3.2 are satisfied. Then, the following algorithm can be applied. A summary of the proposed SMO-based state estimation and attack detection is shown in Fig. 3.3 and Algorithm 3.1. To quantify the operational complexity of the scheme, Table 3.1 presents the number of additions and multiplications required to implement the algorithm. The implementation requires a total of 257 multiplications and 148 additions, of which only 23 multiplications and 14 additions are performed online; the remaining computations are executed offline, further minimizing the real-time computational burden.

3.3 Control system design

This section discusses control system design, including secondary and primary controllers, which stabilize the under-study MG, ensuring proportional current sharing and accurate voltage balancing. A primary controller based on two proportional-integral (PI) controllers is used to provide global stability within DGs. However, this control system alone is not able to do this [172]. Thus, a distributed secondary controller based on consensus algorithms is developed to ensure the achievement of MG's objectives. In the sequel, these two controllers have been discussed. Before addressing this

Algorithm 3.1 Proposed SM-based unknown input observer for attack detection

Input: Matrices $\bar{A}$, $\bar{B}_1$, $\bar{B}_2$, $\bar{C}$, and signal $u_1(t)$ and $h(t)$.

if *Condition* 3.1 is not satisfied **then**
    STOP
else
    Construct matrices T and S [using (3.24), (3.28), and (3.29)].
    Compute $\check{A}$, $\check{B}$, and $\check{C}$ with (3.23).
    if *Condition* 3.2 is not satisfied **then**
        STOP
    else
        Construct $\check{L}_{22}$ so that $\left(\check{A}_{22} - \check{L}_{22}\check{C}_{22}\right)$ is Hurwitz.
        Choose a positive definite $\check{Q}_{22}$.
        Solve (3.36) to find $\check{P}_{22}$.
        Choose υ that satisfies (3.43).
        Construct $\check{L}$ and $\check{F}$ via (3.36) and (3.44).
        Compute L and F by (3.37).
        Compute $\mathcal{H}_j(\hat{h}_j - h_j, \eta_j)$ with (3.16).
        Construct the SMO with (3.15).

Table 3.1 . Operational complexity of offline and online parameters

Type	Parameters	Multiplications and Additions
Offline Parameters	T	$55M + 30A$
	S	$26M + 15A$
	$\check{A}$	$54M + 12A$
	$\check{B}_2$	$18M + 18A$
	$\check{C}$	$12M + 6A$
	$\check{L}_{22}$	$6M + 5A$
	$\check{P}_{22}$	$24M + 16A$
	$\check{Q}$	$28M + 26A$
	L	$30M + 18A$
	F	$4M + 2A$
Online Parameters	$\mathcal{H}_j(\hat{h}_j - h_j, \eta_j)$	$2M + 3A$
	SM-based UIO	$21M + 11A$

issue, the following assumption is required.

Assumption 3.3. *It is assumed that the voltage references for all DGs are identical (i.e.,* $v_{dc_j}^{ref} = v_{dc}^{ref}$*, for* $j \in \mathcal{N}_j$*). Otherwise, the voltage of all DGs should converge to the average voltage value (i.e.,* $v_{dc_j}^{ref} = \langle \mathbf{v}_{dc}^{ref} \rangle$*), where vector* $\mathbf{v}_{dc}^{ref} = \left[v_{dc_1}^{ref}, v_{dc_2}^{ref}, \cdots, v_{dc_{\mathcal{N}_j}}^{ref} \right]^T$ *denotes reference voltage of all DGs.*

3.3.1 Secondary control system

A distributed secondary controller based on a consensus algorithm is developed in this section. The consensus algorithm is a common distributed approach for obtaining global information sharing. Since the considered secondary control system has a distributed structure, each DG in any topology must establish communication with only neighboring units.

Definition 3.1. *At the steady state and constant load currents, current sharing among DGs means that the overall load current is proportionally shared among DGs. This definition can be expressed as follows:*

$$\frac{i_{dc_j}}{i^{\alpha}_{dc_j}} = \frac{i_{dc_k}}{i^{\alpha}_{dc_k}} \quad \textit{for all } j,k \in \mathcal{V}, \tag{3.54}$$

where $i^{\alpha}_{dc_j}$ *and* $i^{\alpha}_{dc_k}$ *are constant scaling factors.*

Thus, to adjust the reference voltage value of each DG to guarantee current sharing and voltage balancing, the following voltage correction term for each DG should be calculated in the secondary controller [173].

$$\dot{\Delta} v_{dc_j}(t) = -k_I \sum_{k \in \mathcal{N}_j} a_{jk} \left(\frac{i_{dc_j}}{i^{\alpha}_{dc_j}} - \frac{i_{dc_k}}{i^{\alpha}_{dc_k}} \right), \tag{3.55}$$

Here, $a_{jk} > 0$ when there is a connection between DG_j and DG_k; otherwise, $a_{jk} = 0$. According to this secondary control law, where all neighboring DGs communicate only through current signals, cyber-attacks can affect and manipulate the under-study MG just in this channel. However, the proposed approach can be readily applied to voltage channels as well. After determining this correction term for each DG, the reference voltage value of each DG can be calculated as follows:

$$v^{ref}_{dc_j} = v^{ref}_{dc} + \Delta v_{dc_j}. \tag{3.56}$$

Figure 3.4 shows the structure of this secondary control system, where a consensus scheme is adopted to adjust the references of each primary voltage control. In this figure, blue block shows the communication topology of all DGs, while yellow block illustrates the implementation of the designed secondary controller, formulated in (3.55). After calculating the correction term (i.e. Δv_{dc_j}), the reference voltage of each DG can be obtained by summing this correction term with the reference voltage of the entire MG, as shown in the green block of this figure. Also, further analysis on this consensus-based secondary controller can be found in [173].

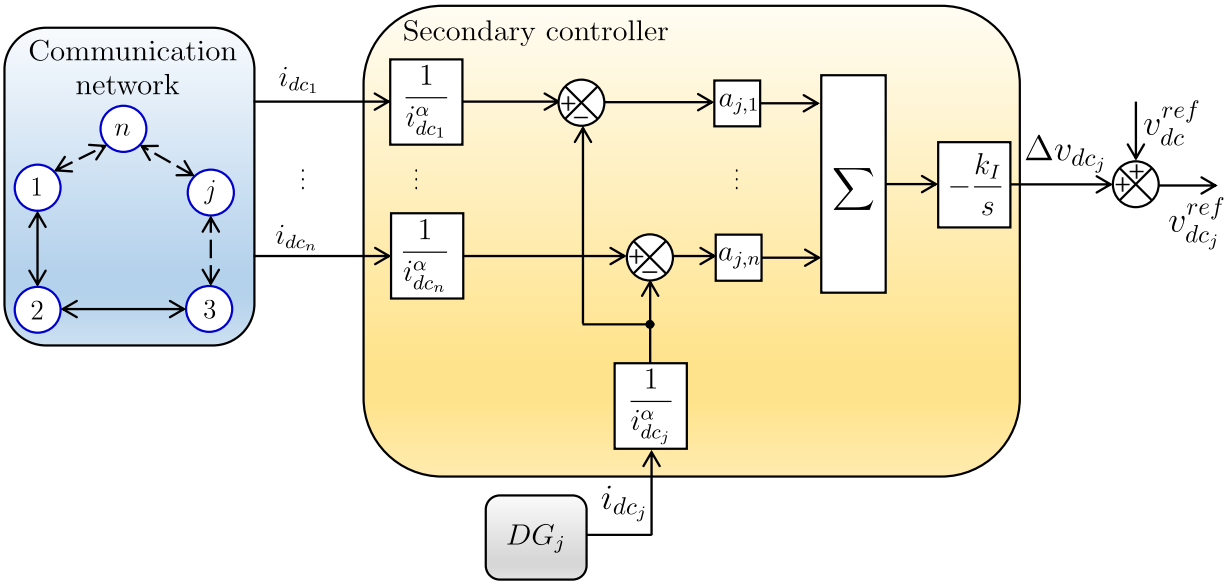


Figure 3.4 . Consensus-based secondary control structure

The secondary controller is complemented by a primary controller, which is discussed further in the next subsection.

3.3.2 Primary control system

As aforementioned, after designing the secondary controller, which determines the reference voltage value for all DGs, a primary controller should be designed to secure the attainment of dc MG's objectives. Therefore, by designing two PI controllers for each DG, their current and voltage will be regulated. To design these controllers, the following transfer functions of the considered dc MG can be presented:

$$\begin{aligned} \frac{i_{dc_j}(s)}{v_{t_j}(s) - v_{dc_j}(s)} &= \frac{1}{l_{f_j}s + r_{f_j}}, \\ \frac{v_{dc_j}(s)}{i_{dc_j}(s) - i_{O_j}(s)} &= \frac{1}{c_{f_j}s + 1/r_j}, \end{aligned} \tag{3.57}$$

where i_{O_j} denotes the output current from DG_j. Figure 3.5 shows the structure of these primary controllers. These controller's gains are selected as follows:

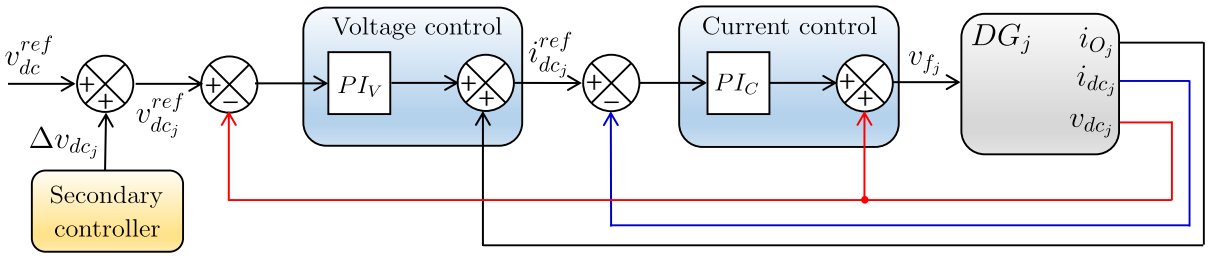


Figure 3.5 . The structure of the designed primary control system.

$$\begin{aligned} k_{i_V} &= c_{f_j}(\omega_n/10)^2 \quad & k_{p_V} &= 2\zeta(\omega_n/10)c_{f_j} - 1/r_j, \\ k_{i_C} &= \omega_n^2 l_{f_j} & k_{p_C} &= 2\zeta\omega_n l_{f_j} - r_{f_j}, \end{aligned} \tag{3.58}$$

where k_{i_V}, k_{p_V}, k_{i_C}, and k_{p_C} denote the integral and proportional gains of PI controllers. It's worth noting that the main reason for the speed of the voltage controller, which is one-tenth of that for the current control, is to avoid the interaction of fast and slow dynamics of the inner and outer loops [174]. In the following, it is shown that the designed primary and secondary controllers, along with the proposed SM-based UIO scheme, can provide the following objectives in the dc MG against FDIAs [3].

$$\begin{aligned} & v_{dc_j}^{ref} = \langle \boldsymbol{v}_{dc}^{ref} \rangle, \\ & \frac{i_{dc_j}}{i_{dc_j}^{\alpha}} = \frac{i_{dc_k}}{i_{dc_k}^{\alpha}} \quad \text{for all } j,k \in \mathcal{V}, \end{aligned} \tag{3.59}$$

where $\langle \boldsymbol{v}_{dc}^{ref} \rangle$ has been defined in *Assumption* 3.3. Section 3.4 illustrates the ability of the proposed method to provide the desired safe operation of dc MGs in the presence of various FDI cyber-attacks.

Cybersecurity is strengthened through the deployment of observer-based detection methods, which may introduce additional communication overhead, particularly when real-time state estimation or control signal updates are required. These methods may require frequent data exchange between distributed units or between sensors and a centralized detector/controller, thereby increasing bandwidth usage and imposing stricter latency requirements. However, this trade-off is managed in the following ways:

1. The observer is designed to function with limited transmitted data, minimizing the need for frequent global communication. In the proposed scheme, only current signals are transmitted, significantly reducing the overall communication burden.

2. The latency tolerance of the proposed scheme will be evaluated through simulation, and the results indicate that the method maintains stability and detection performance even under moderate communication delays.

Ultimately, while the proposed method introduces modest communication demands, these are justified by the significant improvements in detection accuracy and system resilience to cyberattacks.

3.4 Results and discussions

The efficacy of the proposed attack detection and mitigation scheme is evaluated under diverse conditions, such as the MG parameter uncertainty, local load changes, and different FDIA behaviors. It is worth noting that all simulations are conducted on OPAL-RT real-time simulator.

3.4.1 Performance evaluation of the proposed scheme

This subsection is devoted to the efficiency evaluation of the proposed cybersecurity approach. For this purpose, a six-DG dc MG connected with resistive power lines is studied with the OPAL-RT real-time simulator. The architecture of this setup, which is composed of OPAL-RT, a laptop, a router, and an oscilloscope, is shown in Fig. 3.6(a). This host computer is an asynchronous subsystem that will act as a user interface. Figure 3.6(b) depicts the schematic of this MG. It is assumed that the capacity of even DGs (i.e., DG_2, DG_4, and DG_6) is twice the capacity of odd DGs (i.e., DG_1, DG_3, and DG_5). Figure 3.6(c) shows the capacity of each DG. In addition, the considered MG parameter values are summarised in Table 3.3. In addition, the power line resistances and inductance are selected as $r_{12} = 0.36\ \Omega$, $r_{13} = 0.5\ \Omega$, $r_{24} = 0.55\ \Omega$, $r_{34} = 0.4\ \Omega$, $r_{45} = 0.45\ \Omega$, $r_{56} = 0.3\ \Omega$, $r_{16} = 0.6\ \Omega$, $l_{12} = 10\ \mu$H, $l_{13} = 20\ \mu$H, $l_{24} = 25\ \mu$H, $l_{34} = 50\ \mu$H, $l_{45} = 40\ \mu$H, $l_{56} = 30\ \mu$H, and $l_{16} = 15\ \mu$H. Moreover, the parameters' value of the proposed observer are provided in Table 3.2.

In this case study, we consider $v_{dc}^{ref} = 320$ V. Intending to show the performance of the designed secondary and primary control systems in providing stability and achieving the desired objectives, they are applied to the six-DG dc MG in the absence of cyber-attacks. According to the voltage and current of all DGs shown in Fig. 3.7(a), they can provide proportional current sharing and accurate voltage regulation. Nonetheless, it is inevitable to encounter unfavorable conditions, such as cyber-attacks, parameter uncertainties, measurement noise, and external disturbances. For this purpose, Fig. 3.7(b) depicts the currents and voltages of all DGs against FDIA when the proposed

Table 3.2 . Parameter values used for designing the proposed UIO-based attack detection

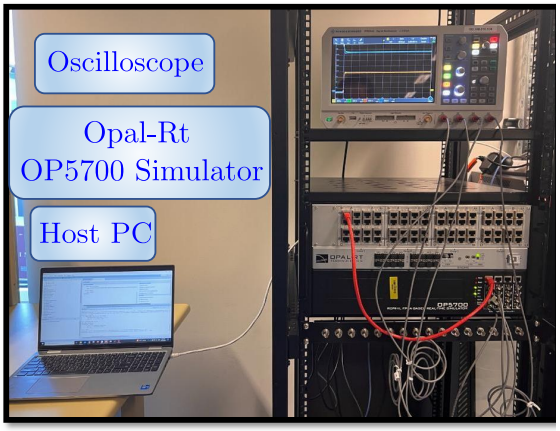
Parameter	Value	Parameter	Value
T_s	50 μs	η	1500
υ	100	k_I	10
i_{dc}^{α}	1 for odd and 2 for even DGs	$\check{Q}_{22}$	I_2

attack detection and mitigation are not applied. As was expected, the desired objectives were not achieved, i.e., (3.59) is not fulfilled. As shown, following the attacks at $t = 1$ s, 2 s, and 3 s, the voltages and currents of all DGs are significantly affected and lose regulation. This indicates that the desired operational objectives of the under-study dc MG are violated under cyberattack conditions. It confirms the necessity and importance of developing cybersecurity schemes. In this simulation, three FDIAs are applied to the communication links of DG_1 and its neighbors, including a constant FDIA at $t = 1$s, a constant FDIA at $t = 2$s, and a constant FDIA at $t = 3$s to DG_2, DG_3, and DG_6, respectively.

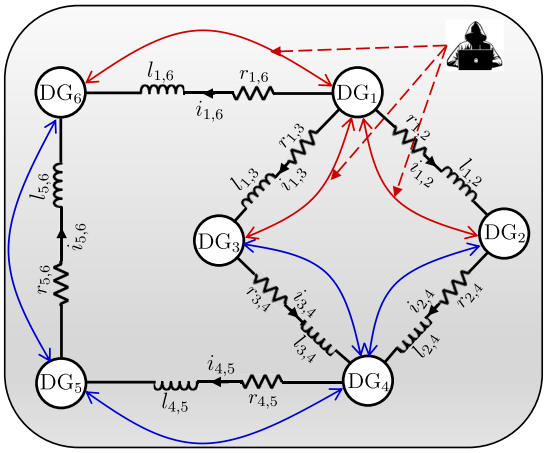
After observing the FDIA consequences on the dc MG in the absence of a proper detection and mitigation mechanism, the proposed strategy is applied to detect and remove the FDIA effects. By implementing *Algorithm* 1, T and S are obtained. According to Fig. 3.8, it is evident that the proposed SM-based UIO can successfully detect and mitigate FDIAs, which confirms the effectiveness of the proposed method in dealing with FDIAs. Thus, (3.59) is fulfilled. In addition, the actual profile of FDIAs and their estimated ones are shown in Fig. 3.9, which shows that the proposed approach can reconstruct attacks effectively.

3.4.2 Robustness evaluation against MG parameters uncertainty

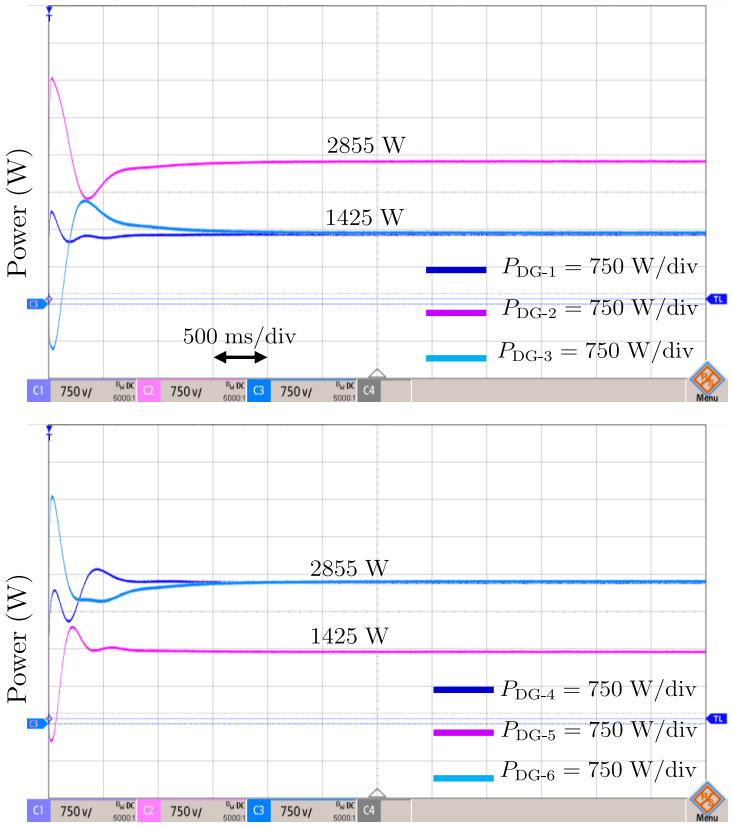
In this section, a parameter uncertainty analysis is conducted to assess the robustness of the proposed attack detection and mitigation strategy. It is worth noting that the dc MG parameters, including the shunt capacitor, filter inductance and resistance, as well as the power lines resistance, cannot be easily computed. As a result, their actual values might be different from the opted ones for the designed observer. Thus, it is necessary to investigate the sensitivity of the proposed method to these parameters to validate its effectiveness [175].



(a)



(b)



(c)

Figure 3.6 . **(a)**. The real-time setup, **(b)**. The considered dc MG, and **(c)**. Power of each DG

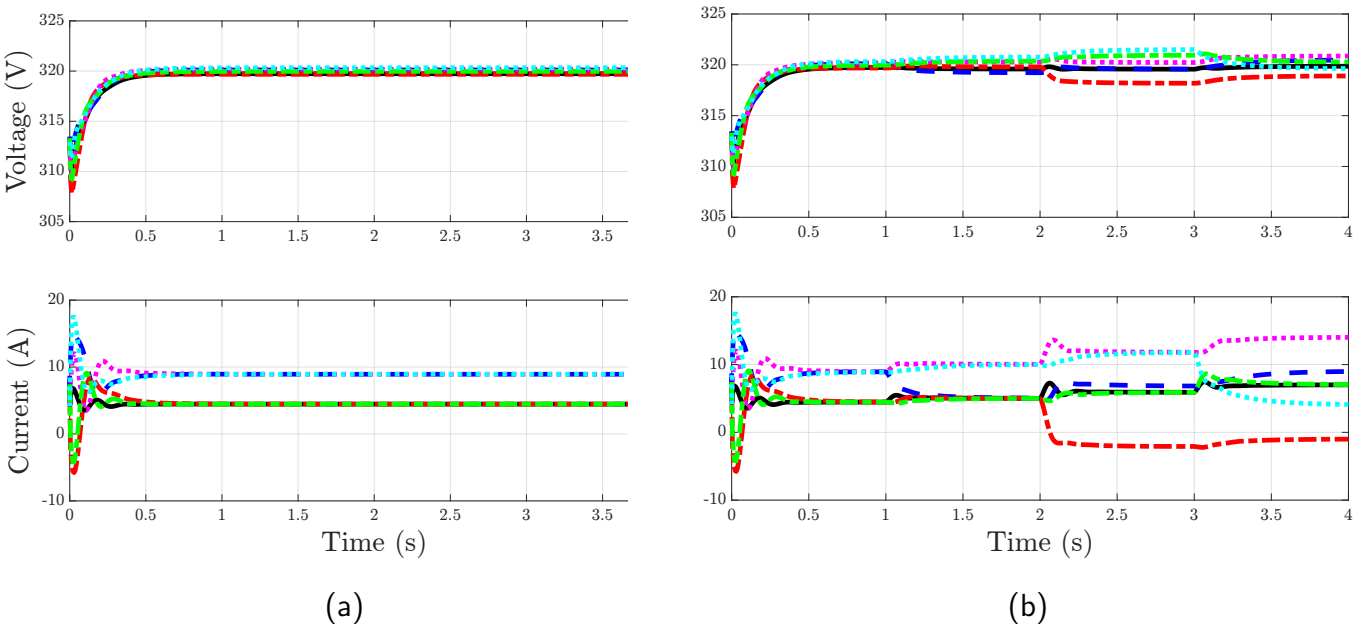


Figure 3.7 . The values of voltages/currents **(a)**. for all DGs in the absence of FDIAs, **(b)**. for the compromised MG without any attack detection/mitigation mechanism.

Table 3.3 . Parameters of the six-DG MG for simulations

Unit \ Symbol	r_{f_j} (Ω)	l_{f_j} $(m\text{H})$	c_{f_j} $(m\text{F})$	r_j (Ω)
DG_1	1	2.5	3.5	50
DG_2	0.75	3	5	40
DG_3	1.2	3.5	2	55
DG_4	1.1	2	4	45
DG_5	0.9	4	2.5	52
DG_6	1.5	4.5	4.5	48

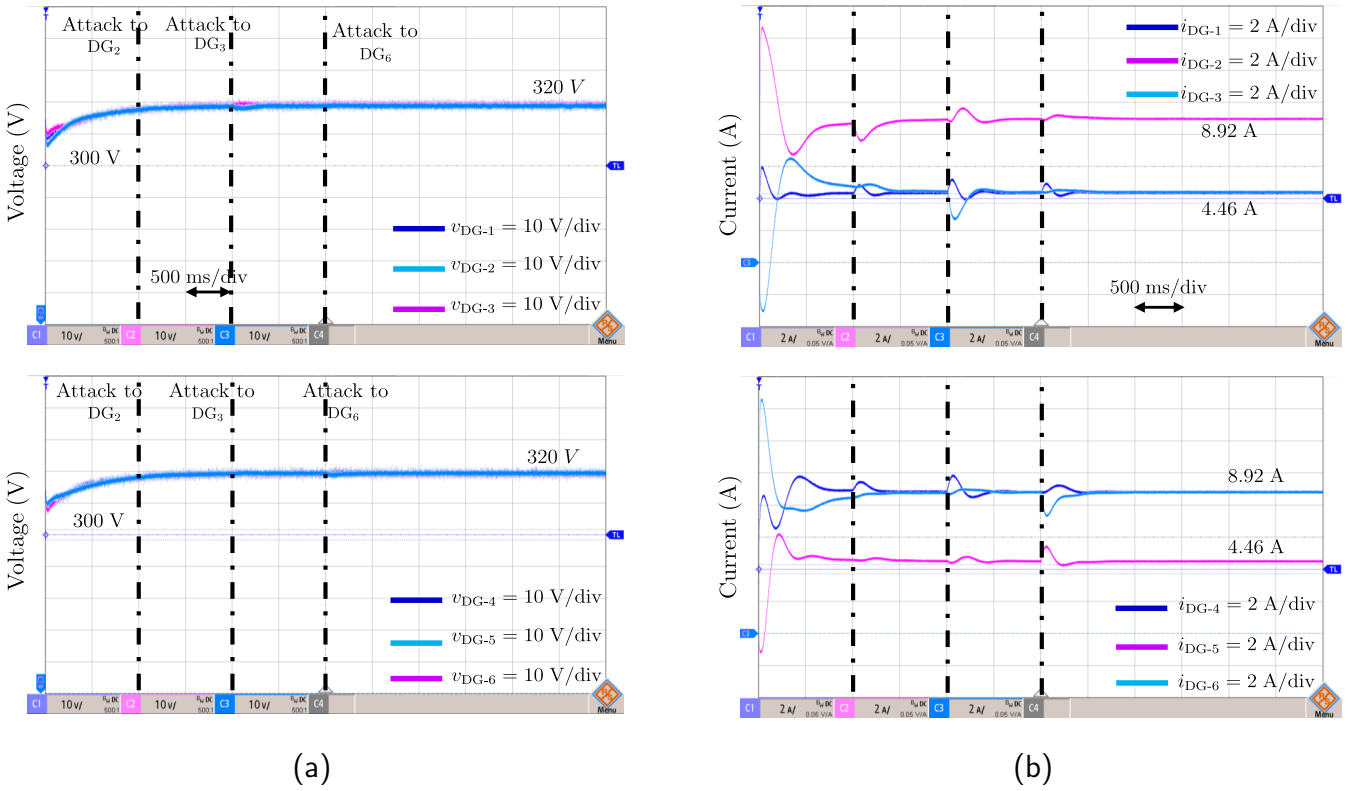


Figure 3.8 . The values of **(a).** voltages and **(b).** currents for all DGs against constant FDIAs with the proposed attack detection/mitigation mechanism.

For this purpose, the physical parameters of the power lines, i.e., resistance and inductance of the lines, are increased by 15%, 30%, and 40%, while the physical parameters of DGs, i.e., filter inductance, resistance, and shunt capacitor, are decreased by 15%, 30%, and 40%. In should be noted that it is assumed that the capacity of all DGs are equal. Moreover, two FDIAs are applied to the communication links of DG_3 and its neighbors, including a constant FDIA at $t = 1$s, and a constant FDIA at $t = 2$s to DG_1 and DG_4, respectively. Figure 3.10 shows the voltage and current of each DG in the presence of different dc MG parameter values. As it is obvious, the voltages and currents of all DGs for different parameter values do not show any noticeable differences from the corresponding output for the nominal parameters. This confirms that the proposed SM-based UIO for attack detection is effective even when there is an uncertainty in the parameters which confirms the applicability to real-world dc MGs with high uncertainties. Due to the inherent robustness that

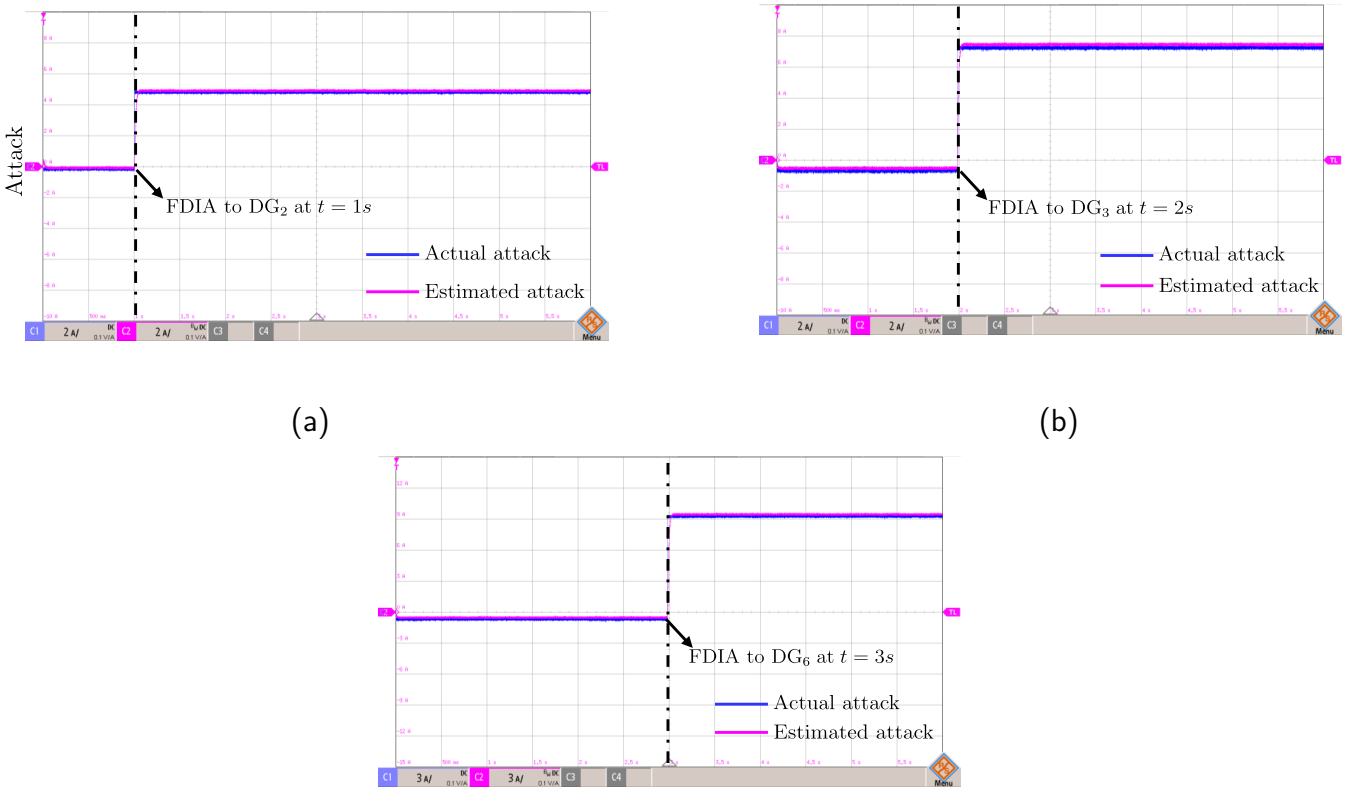


Figure 3.9 . FDIA detection with the proposed SM-based UIO strategy, **(a)**. DG_2, **(b)**. DG_3, and **(c)**. DG_6.

the SMO technique has against uncertainties, it was expected that this method would show this behavior against the parameter uncertainties.

3.4.3 Performance evaluation against DoS attacks

In this section, the performance of our proposed attack detection/mitigation has been evaluated against a kind of DoS attacks. To model this DoS attack, the signal generated by the physical layer is passed to the cyber layer for sending, where the attacker endeavors to disrupt the transmission to the receiver using the DoS attack [176]. The system under this attack can be represented by the subsequent model.

$$y_k = Cx_k + \Psi\ell_k, \tag{3.60}$$

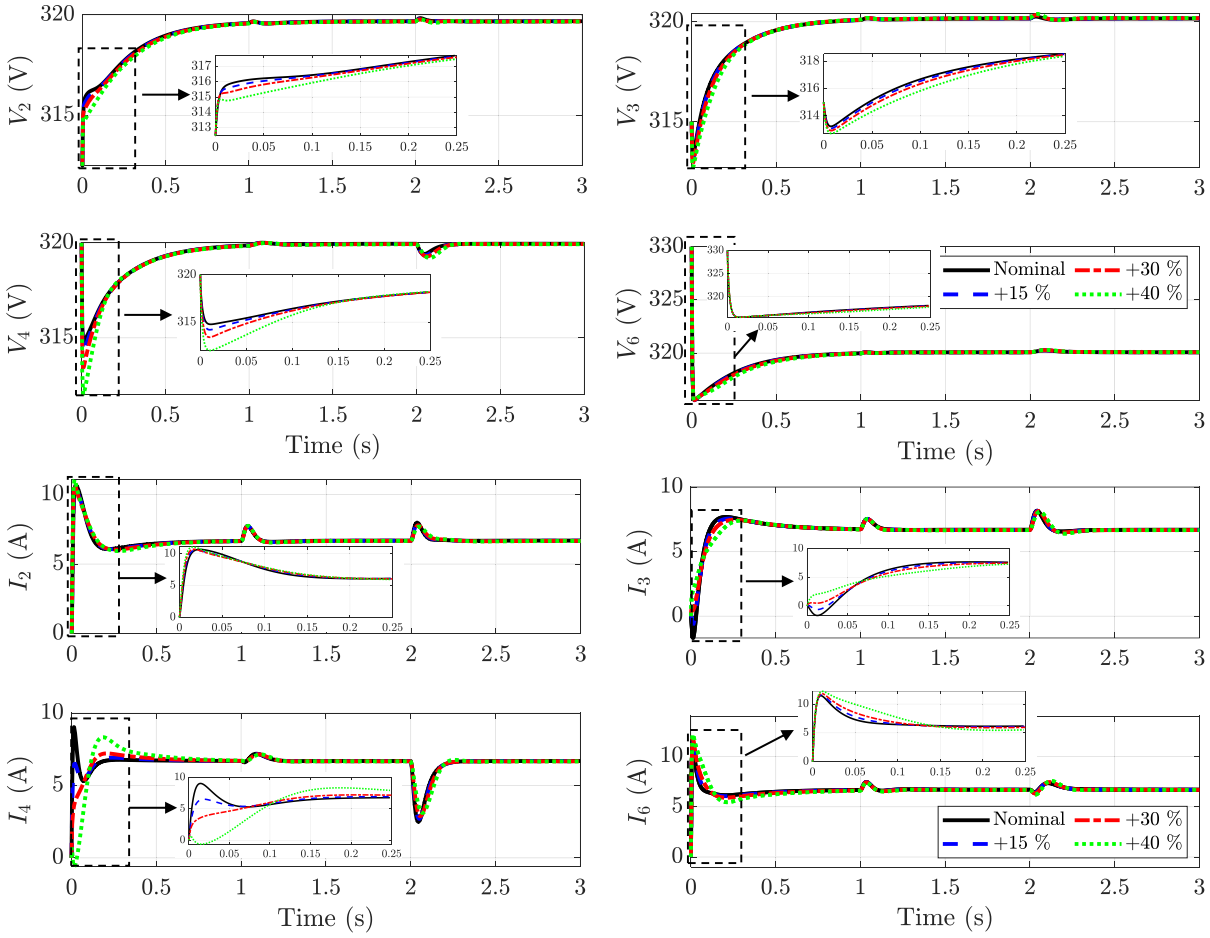


Figure 3.10 . Uncertainty analysis on physical parameters of DGs and power lines.

where $\Psi\ell_k$ is the attack term. More detailed, Ψ is the attack function while ℓ_k represents the time that attack is launched. The attacker launches a DoS attack for the output signal y_k to offset the right signal in the period $[k_s, k_e]$, where k_s means the start time of the attack and k_e represents the end time. The progress can be formulated as

$$\begin{cases} \Psi = C, \\ \ell_k = -x_k, k \in [k_s, k_e], \\ \ell_k = 0, k \notin [k_s, k_e]. \end{cases} \tag{3.61}$$

Substitute (3.61) into (3.60), which can be further written as:

$$\begin{cases} y_k = 0, \quad k \in [k_s, k_e], \\ y_k = Gx_k, \quad k \notin [k_s, k_e]. \end{cases} \tag{3.62}$$

Thus, DoS attacks can be formulated. In the following, the effectiveness of the proposed attack detection/mitigation technique against the DoS attack has been illustrated. In this regard, two DoS attacks have been applied to DG_2 and DG_3 from $t = 1$s to $t = 2$s and $t = 2.5$s to $t = 3$s, respectively. Figure 3.11 depicts the voltages and currents of all DGs in the presence of DoS attack. As is clear, in the absence of our proposed SM-based UIO method, the desired dc objectives have not been achieved. During the attack on the current communication channels, the system's dynamic behavior is noticeably disturbed, particularly between $t = 1$ s to 2 s and $t = 2.5$ s to 3 s. However, upon activation of the proposed scheme, the attacks are promptly detected and mitigated, resulting in minimal impact on the system's dynamic response, which can be observed in Fig. 3.12. This figure shows the effectiveness of this scheme in dealing with DoS attacks. As is evident, (3.59) is fulfilled.

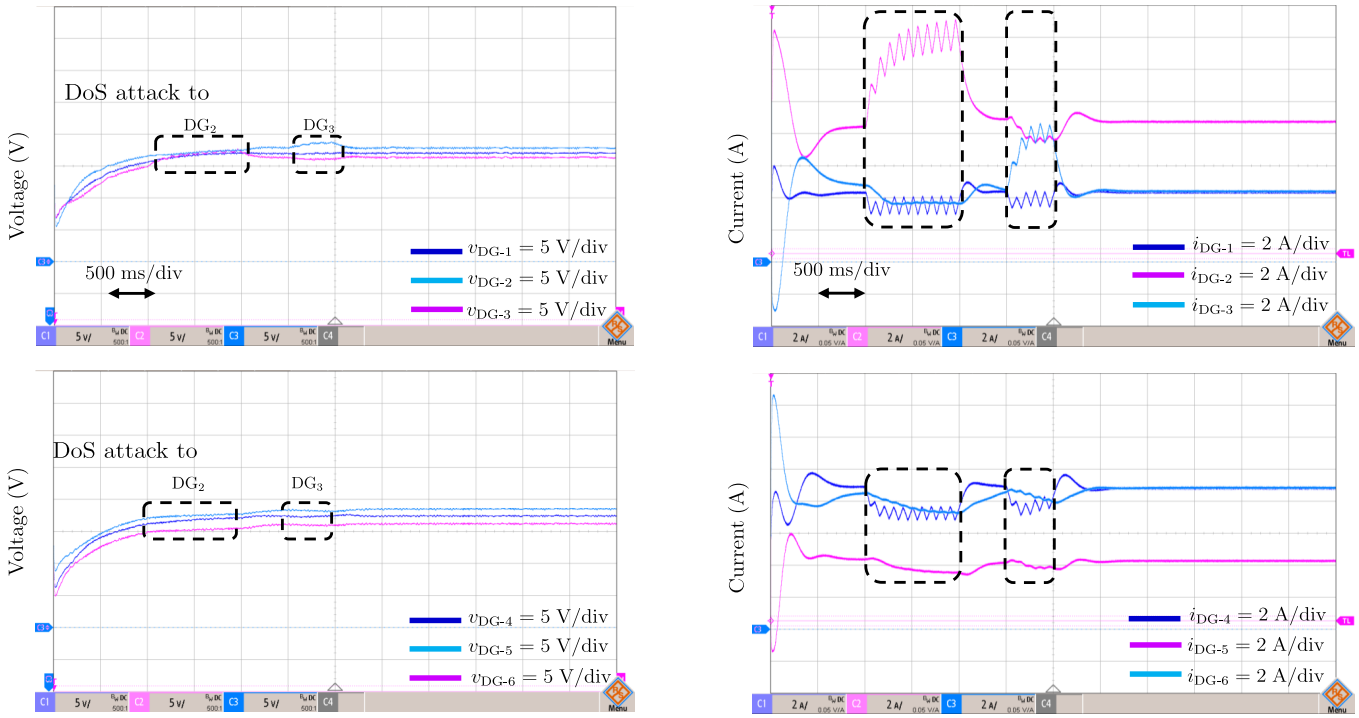


Figure 3.11 . The values of **(a).** voltages and **(b).** currents for all DGs against DoS attack without the proposed attack detection/mitigation scheme.

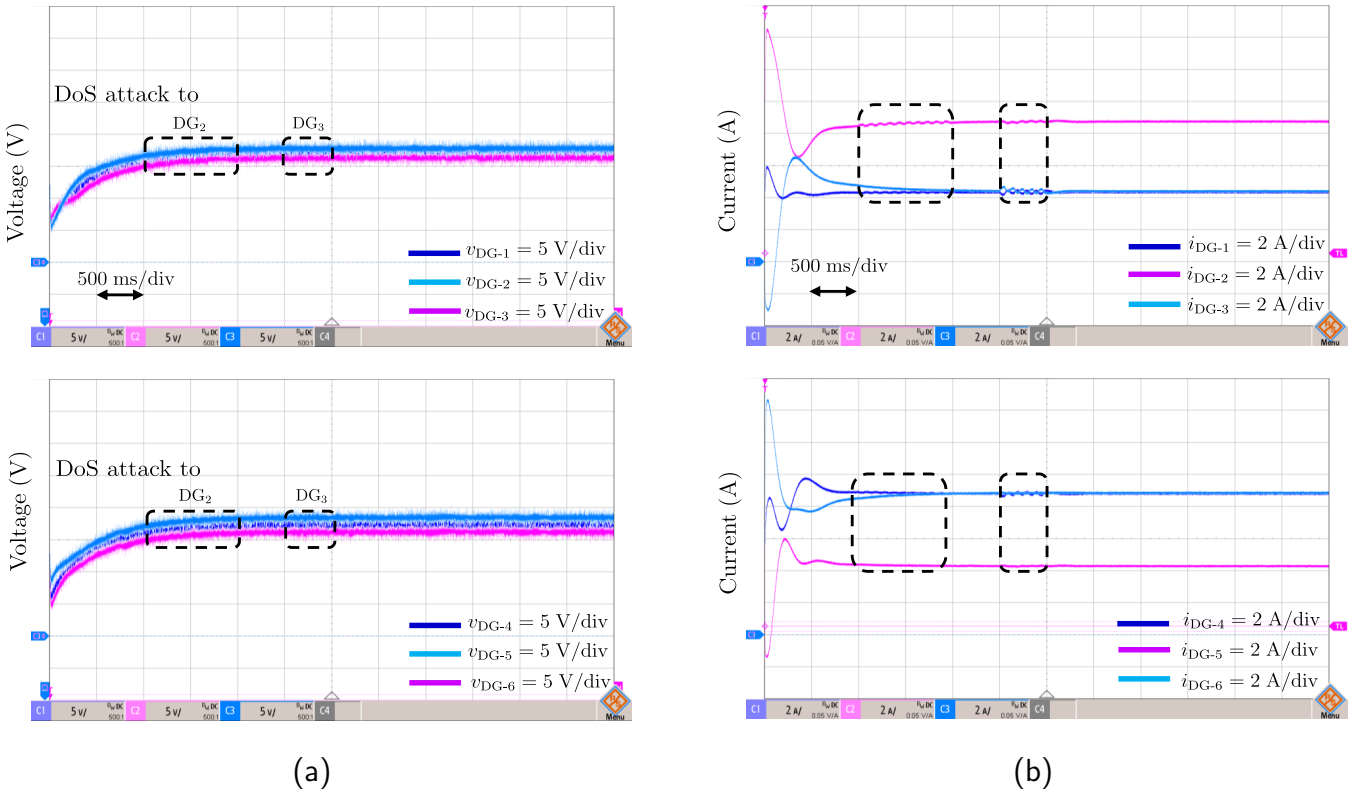


Figure 3.12 . The values of **(a).** voltages and **(b).** currents for all DGs against DoS attack with the proposed scheme.

3.4.4 Performance evaluation against renewable energy resources

As another case study, the model of under-study dc MG has been updated with a renewable energy source. For this aim, DG_2 has been substituted from a simple controlled voltage source to a photovoltaic (PV) panel to investigate the under-study dc MG against various dynamic condition changes. In this regard, Fig. 3.13(a) shows the solar irradiance profile of the PV, by which the PV power is obtained. It should be noted that the power of PV panels in DG_2 is determined according to the temperature and irradiance of the environment and using the maximum power point tracking algorithm. As evident from Fig. 3.13(b), the power of DG_2 is increased by increasing the irradiance, which results in decreasing the power of all other DGs. Therefore, the power of this DG is expected to be imposed externally, while the power of all other DGs is determined and shared according to the designed secondary controller.

In this scenario, two FDIAs are applied to the communication links of DG_2 and its neighbors, including a constant FDIA at $t = 1$ s, and a constant FDIA at $t = 2$ s to DG_1 and DG_4, respectively. Moreover, to mimic the real-world scenarios, the time-delay equals to 5 μ s in the communication links have also been taken into account. In the following, the dynamic response of the dc MG, including the voltage and current of all DGs have been depicted. As was expected, when the input power of the PV panels increases, the power of all other DGs should decrease. According to Fig. 3.14 at $t = 1.5$ s and $t = 3$ s, it is can be seen that the power all other DGs, expect DG_2, decreased and shared equally. Moreover, the proposed scheme can deal with the applied cyber-attacks in the communication channels at $t = 1$ and $t = 2$s to DG_1 and DG_4, respectively. As a result, the applicability of this scheme in more complex MGs can be confirmed.

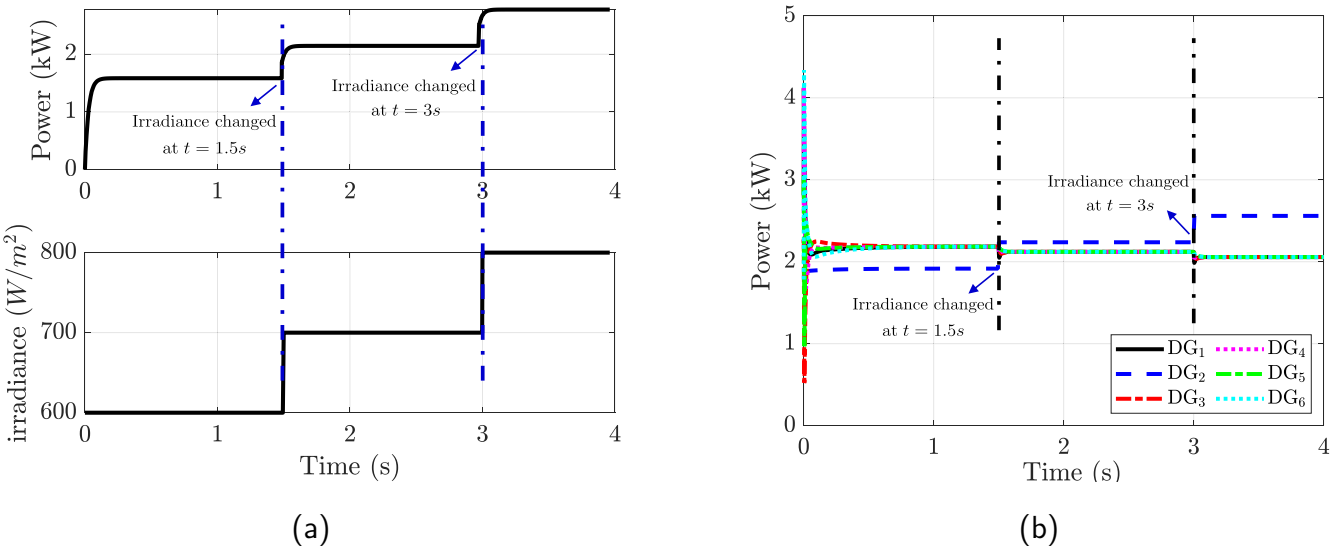


Figure 3.13 . **(a).** PV power and its irradiance profile, **(b).** The power of all DGs.

3.4.5 Performance evaluation against time-varying FDIAs

In this section, the performance of the proposed SM-based UIO scheme against time-varying FDIAs has been evaluated. In this regard, three time-varying FDIAs are applied to the communication links of DG_1 and its neighbors, including a sinusoidal FDIA at $t = 1$s, a ramp FDIA at $t = 2$s, and another FDIA to DG_2, DG_3, and DG_6, respectively. These time-varying attack signals

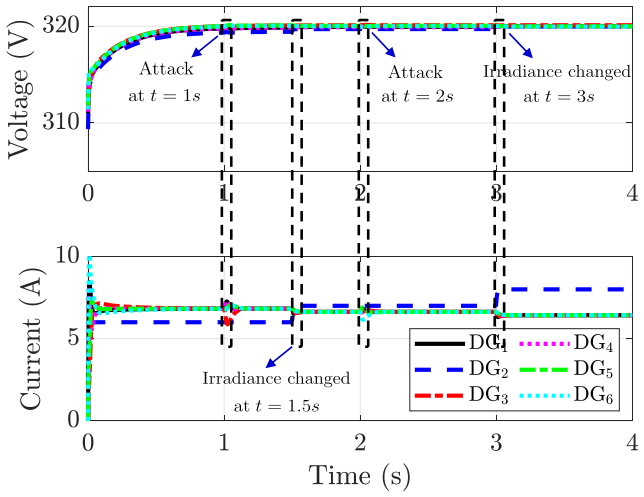


Figure 3.14 . The values of voltages/currents for all DGs with a renewable energy source.

are formulated as follows:

$$a_{1-2} = \begin{cases} 0 & t < 1 \\ 5\sin(7.5t) & t \geq 1 \end{cases}, \quad a_{1-3} = \begin{cases} 0 & t < 2 \\ 12t & t \geq 2 \end{cases}, \quad a_{1-6} = \begin{cases} 0 & t < 1.5 \\ 5t - 7.5 & 1.5 \leq t < 3 \\ -5t + 22.5 & 3 \leq t < 4.5 \\ 0 & t \geq 4.5 \end{cases}. \tag{3.63}$$

In order to show the effectiveness of the proposed method, Fig. 3.15 illustrates the dynamic response of the under-study dc MG against time-varying and unbounded attacks without the proposed technique. The desired objectives (i.e., (3.59)) are not achieved. According to Fig. 3.16, the proposed method can successfully detect time-varying and unbounded FDIAs, confirming this scheme's generality in dealing with different kinds of attacks. In addition, the actual profiles of time-varying FDIAs and their estimates are shown in Fig. 3.17, demonstrating that the proposed approach can effectively detect attacks with different dynamics. To provide a quantitative error metric, the Root Mean Square Error (RMSE) is calculated as follows.

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(x_1(i) - x_2(i)\right)^2} \tag{3.64}$$

The RMSE values of 0.4753, 2.3834, and 0.0071 for the respective attack estimations (DG_2, DG_3, and DG_6) demonstrate the high accuracy of the proposed scheme in detecting cyber-attacks.

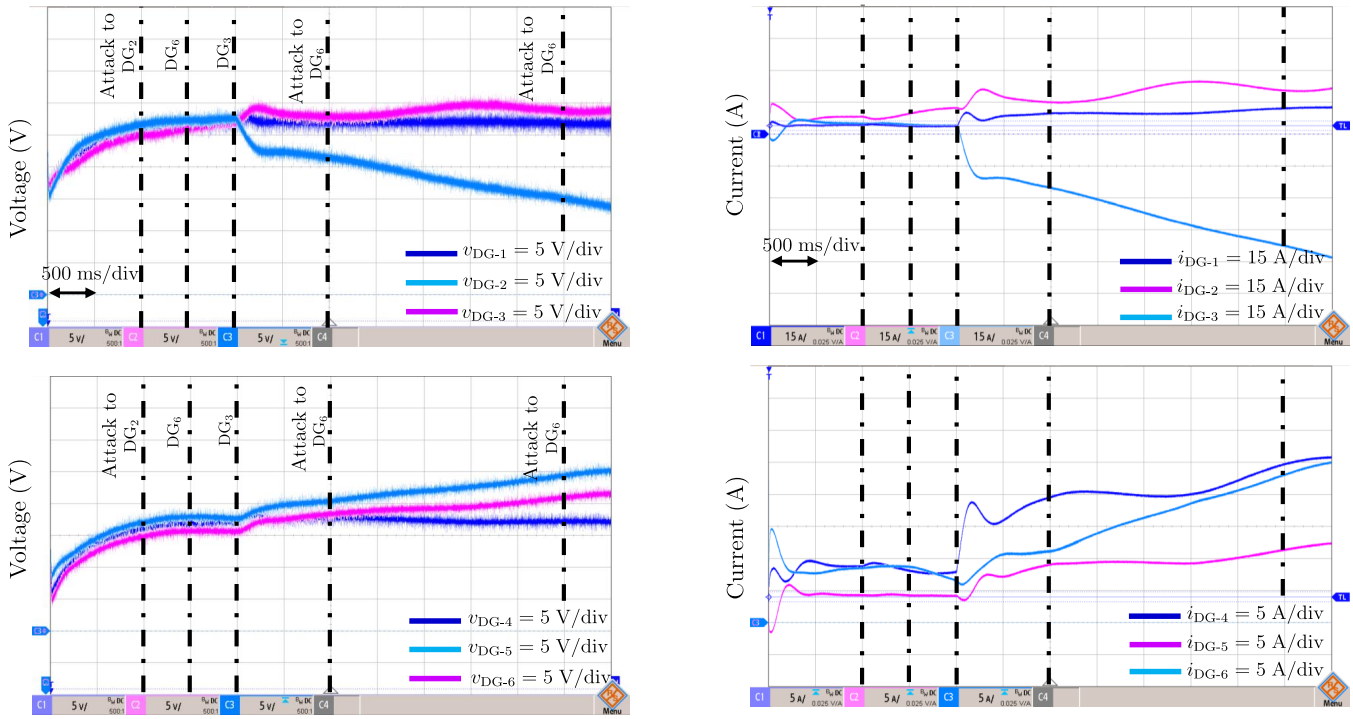


Figure 3.15 . The values of **(a).** voltages and **(b).** currents for all DGs against time-varying and unbounded FDIAs without the proposed attack detection/mitigation scheme.

3.4.6 Long-term stability against evolving grid

In this study, a very general scenario that includes typical cyber-attacks, load changes, and PV information is conducted for a long duration. The details of this scenario are provided as follows:

- FDIAs with constant and time-varying magnitudes are applied to the various DGs of the under-study dc MG. In this regard, three FDIAs are applied to the communication links between DG_1 and DG_4 and their neighbors, including a constant FDIA at $t = 5$s, a time-varying attack at $t = 20$s, and again a constant FDIA at $t = 35$s to DG_2, DG_3, and DG_6, respectively. This is shown with A on the figures.

- It is assumed that the local load of each DG has been changed between $\pm 15\%$ to $\pm 45\%$ at different time instances, including $t = 2.5, 10, 17.5, 25, 32.5$, and 40s. This is shown with B on the figures.

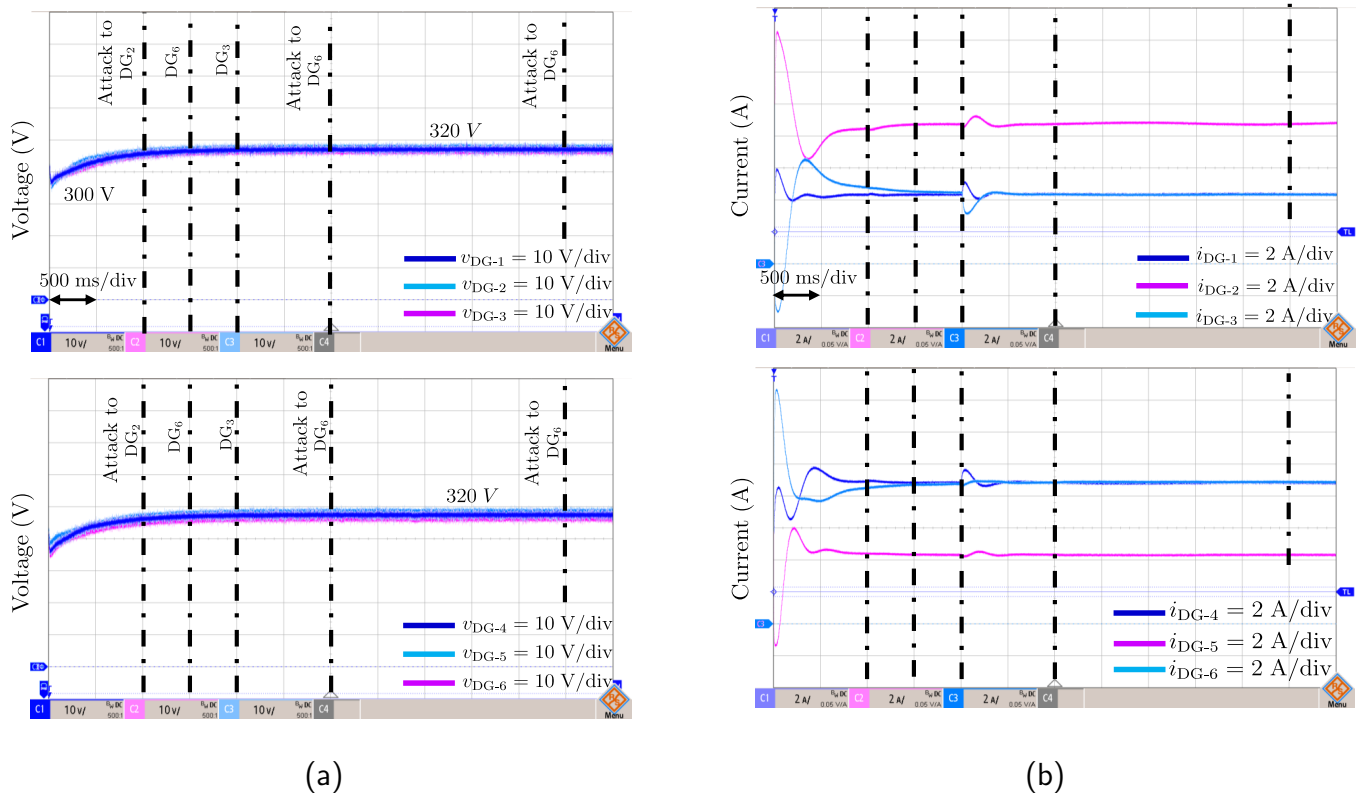


Figure 3.16 . The values of **(a).** voltages and **(b).** currents for all DGs against time-varying and unbounded FDIAs with the proposed scheme.

- The effects of irradiance change, which results in PV generator power change, have also been taken into account. For this purpose, it is assumed that the power generation of DG_5 is changed at $t = 15$ and 30s. This is shown with C on the figures.

Figures 3.18 and 3.19 illustrate the voltage and current of this MG, obtained from real-time simulation. As is apparent, with the proposed observer-based attack detection, the long-term stability and robustness of the dc MG against evolving grid and cyber-attacks are achieved. Figure 3.20 depicts the detection of attack signals by observers situated in adjacent units. Notably, the observers in DG_1 and DG_4 successfully reconstruct the attack signals originating from their neighboring unit, (i.e., DG_3).

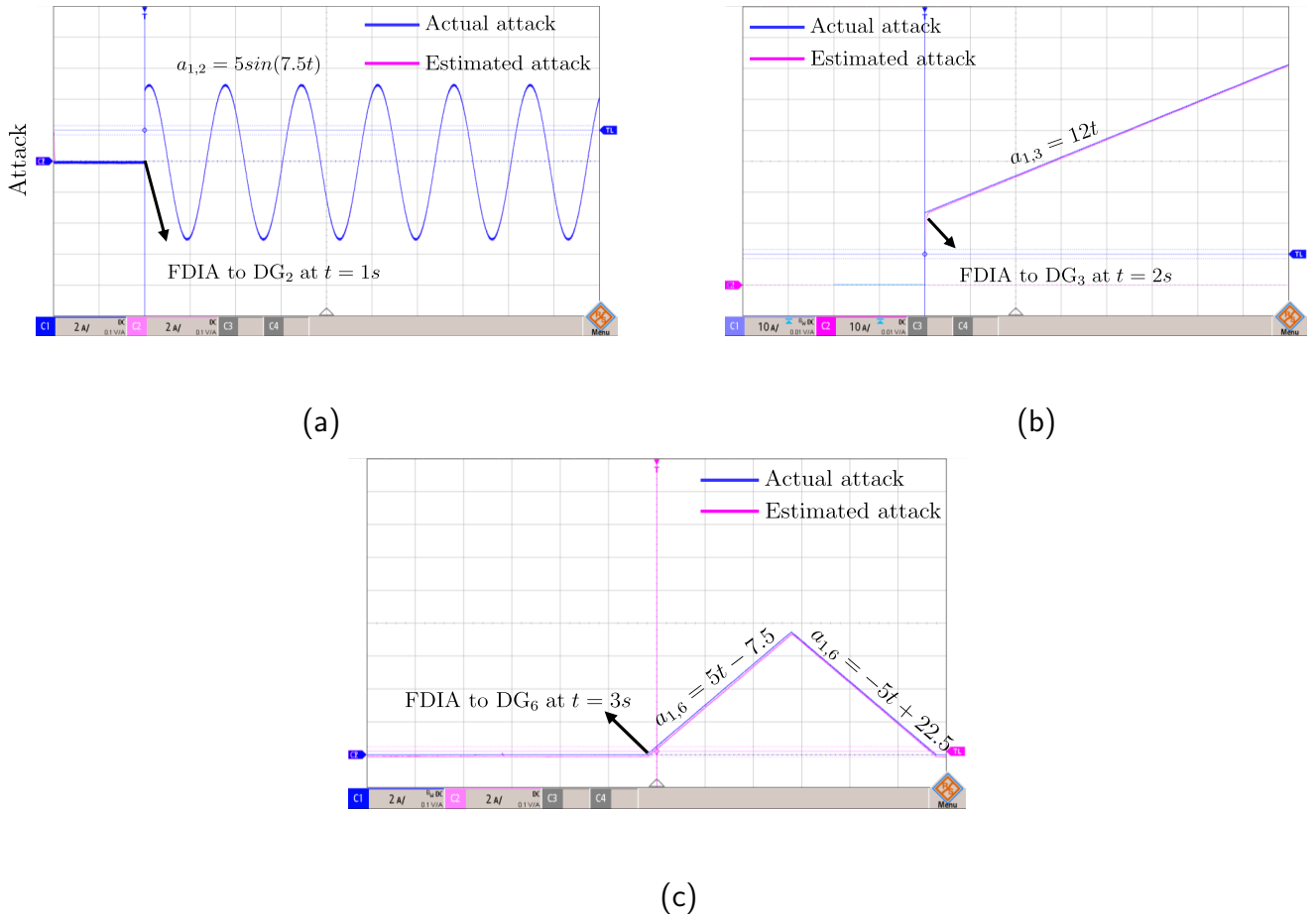


Figure 3.17 . Time-varying FDIA detection with the proposed SM-based UIO strategy, **(a).** DG_2, **(b).** DG_3, and **(c).** DG_6.

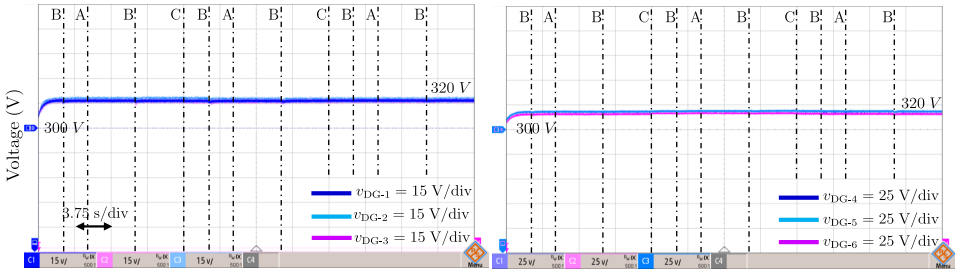


Figure 3.18 . The values of voltages for all DGs against various operation conditions.

3.4.7 Performance evaluation against measurement noise

As was mentioned, noise in the process and measurement sensors is inevitable, degrading the system's performance. We developed a KF to make the transmitted signals noise-free to address

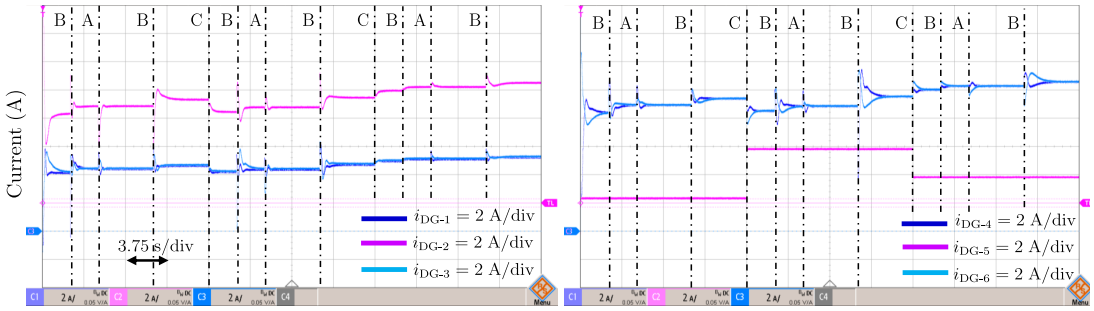


Figure 3.19 . The values of currents for all DGs against various operation conditions.

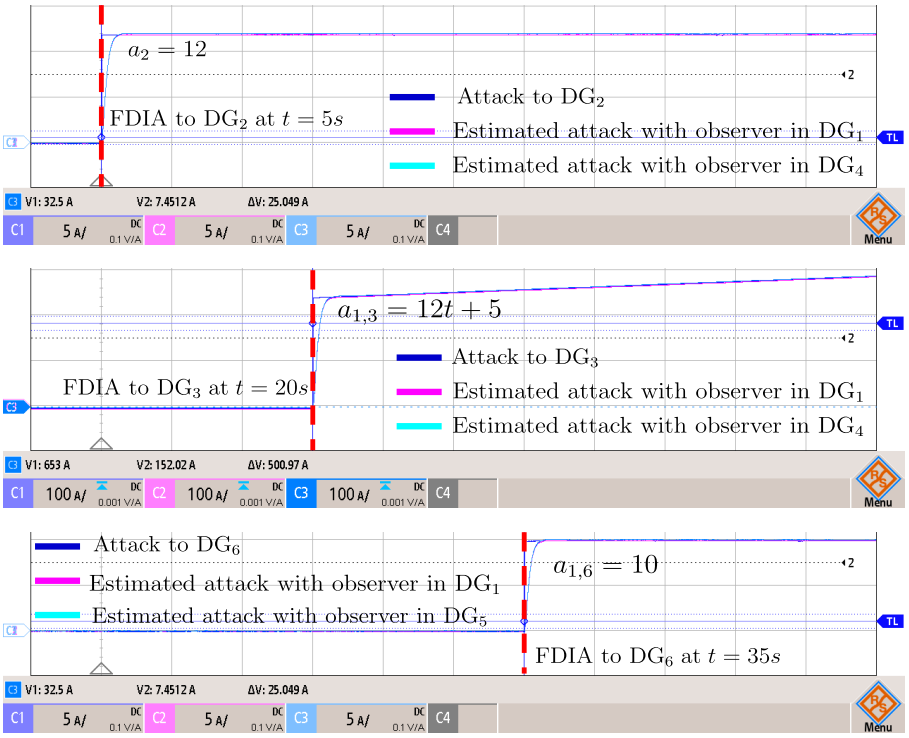


Figure 3.20 . FDIA detection with the proposed SM-based UIO strategy, **(a).** DG_2, **(b).** DG_3, and **(c).** DG_6.

this challenge. In this section, the performance of this filter is evaluated. It is assumed that the sensors of DG_1 are affected by noise. The current signal is affected by high-frequency white noise of variance 0.01. Figure 3.21 illustrates the voltage and current of all units in the presence/absence of the designed KF. As is apparent, with the developed KF, in addition to estimating the states of

local DG, the effects of noise are also canceled out.

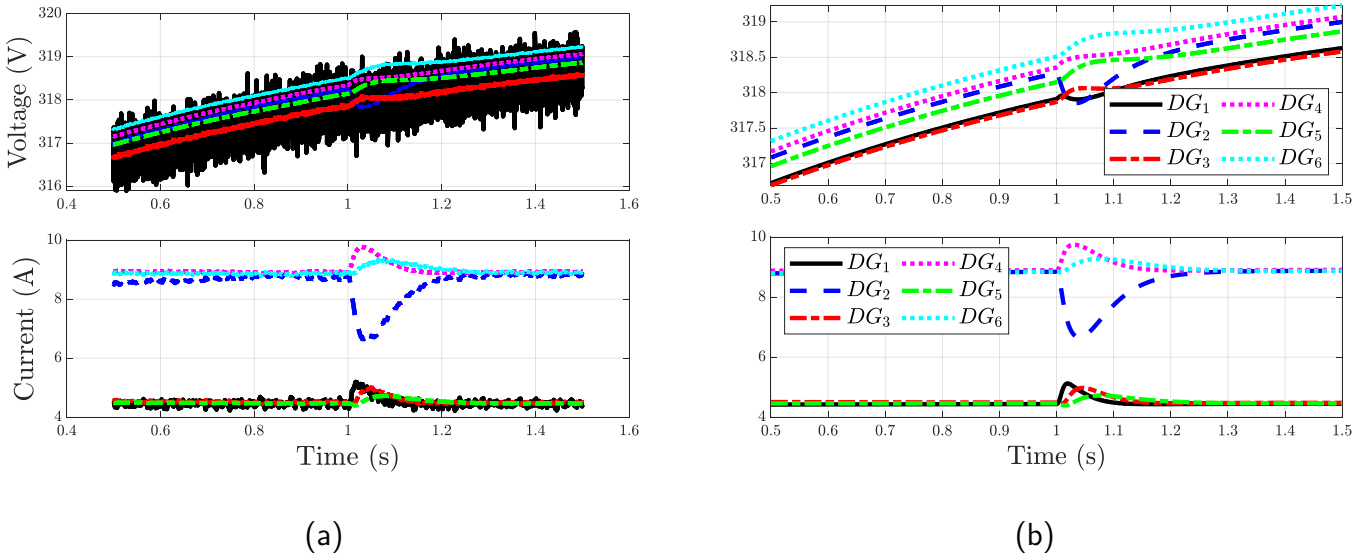


Figure 3.21 . The value of voltage and current of all DGs against FDIA and measurement noise **(a).** without KF and **(b).** with KF.

3.4.8 Scalability assessment

To demonstrate the scalability of the proposed method, simulation results for a dc MG composed of eight DGs with equal capacity are provided. Here, it is assumed that DG_1's neighboring units, DG_2 and DG_8, experience cyber-attacks at times $t = 4$s and $t = 6$s, respectively. The subsequent results illustrate that the proposed observer-based approach can detect and counteract these attacks, thereby reducing their adverse impacts on the system. Figure 3.22 presents the MG configuration alongside the voltage and current readings of all DGs generated with the proposed method.

As illustrated in Fig. 3.22(b), the proposed approach can deal with any dc MG, regardless of the number of DGs. This demonstrates the scalability of the proposed method across various system sizes. Furthermore, the real-time simulation of the studied dc MG using our proposed scheme on the OPAL-RT 5700 simulator achieves an execution time of 0.8 μs with two neighboring units. The simulation's sampling time is 50 μs, highlighting the scheme's capability to effectively reconstruct attacks even when handling a substantial number of neighboring units (approximately 100 DGs).

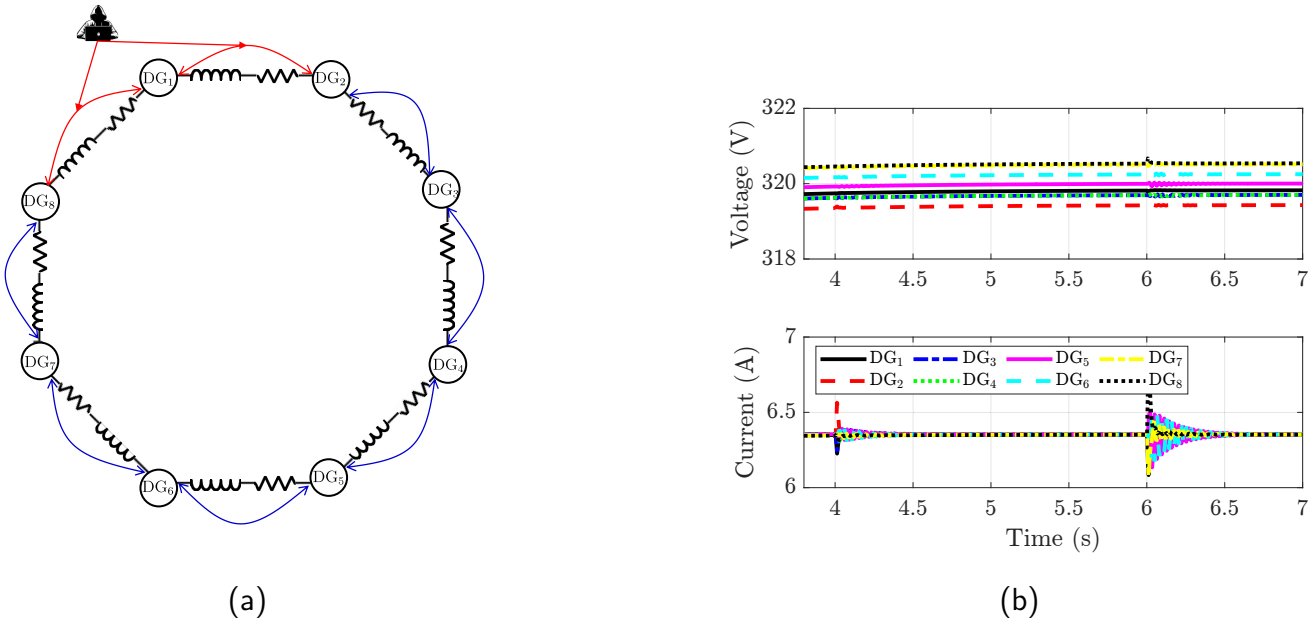


Figure 3.22 . **(a)** The considered dc MG with 8 DGs, **(b)** The values of voltages/currents for all DGs under constant cyber-attacks.

3.4.9 Numerical comparison

In this section, a numerical comparison is conducted between our proposed method and those reported in [2] and [3]. For this purpose, it is assumed that the power output of all DGs is the same. In this study, the physical parameters of the system, as well as the gains of the primary controller for all three methods, are identical. In addition, in [2], all DGs' currents and voltages should be transmitted between neighboring DGs, which can expose the MG to more cyber-attack threats. However, in our approach, it is just required to transmit currents between DGs. To design the observer in [2], we selected $\lambda_0 = 16, \lambda_1 = 121.7$ and $\lambda_2 = 110$. For the high-gain observer proposed in [3], the parameters $\alpha_1, ..., \alpha_{n+1}$ were chosen as $\alpha_1 = 4, \alpha_2 = 6, \alpha_3 = 4$ and $\alpha_4 = 1$. For this observer, $\epsilon = 0.001$, and M was set to 1500, matching the value of η in our proposed method.

As is evident from Fig 3.23, the proposed method can detect cyber-attacks faster than the method developed in [2] and [3], making the adverse and destructive effects of attacks on the system less likely to appear. In this regard, the current and voltage of four DGs of this dc MG has been shown in Fig. 3.24. As is evident, the changes to the current of all DGs, due to the effects of cyber-attacks,

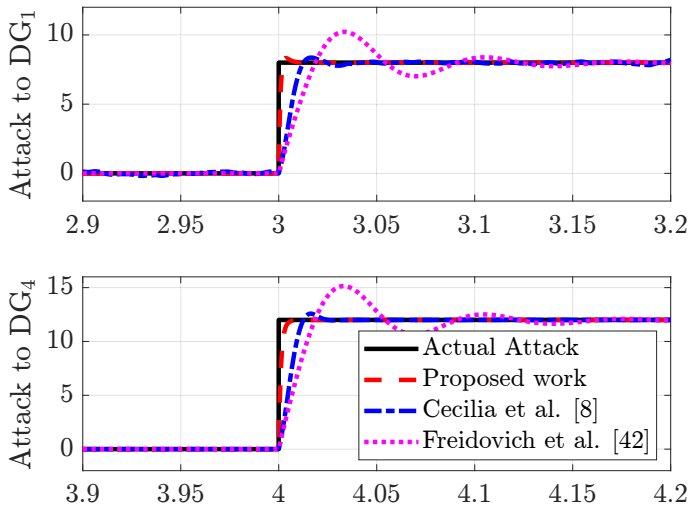


Figure 3.23 . FDIA detection with the proposed method and the one developed in [2] and [3].

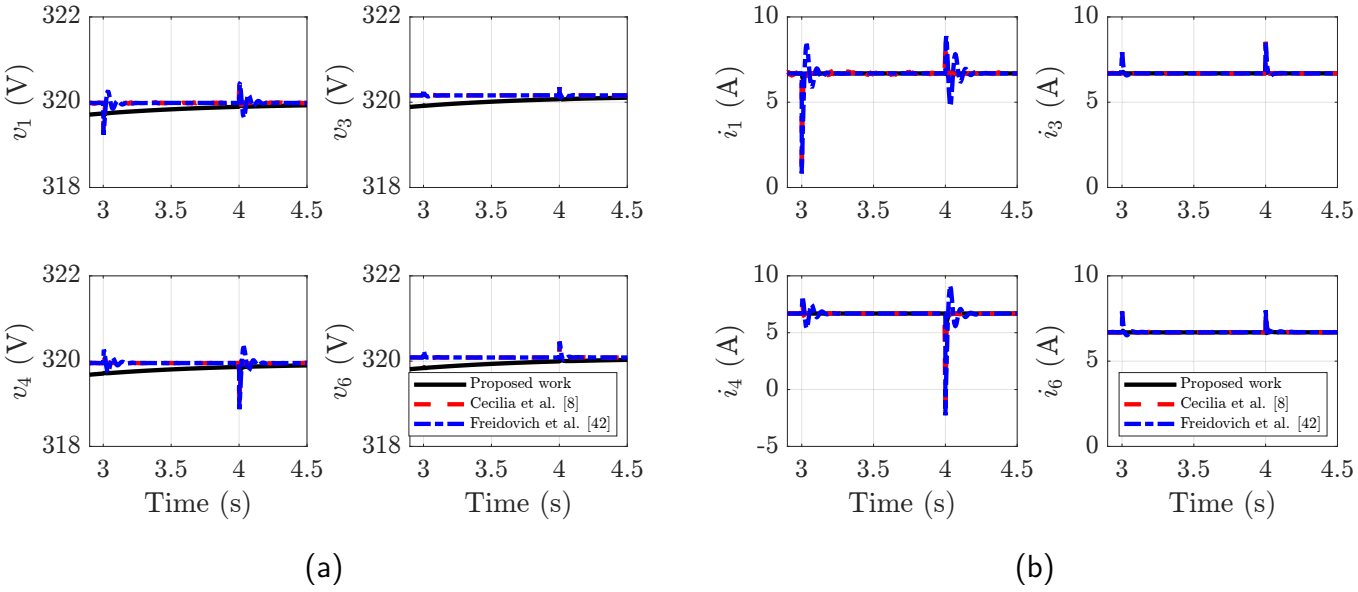


Figure 3.24 . The values of **(a).** voltages and **(b).** currents with the proposed technique and the one developed in [2] and [3].

are much more intense in [2] and [3] compared to the obtained results from our proposed scheme. In this scenario, it is clear that the protection system may be activated in those two methods because the over-current that occurred at the attack instance can lead to relay activation.

It should be noted that the execution time for conducting the real-time simulation of the under-

Table 3.4 . Comparison of Required Computational Time

Method	Proposed SMO-based UIO	Cecilia et al. [2]	Freidovich et al. [3]
Simulation time	0.8μs	1.17μs	1.61μs

study dc MG with our proposed scheme with OPAL-RT 5700 simulator is 0.8 μs, while the required time for the methods proposed in [2] and [3] are 1.17 μs and 1.61 μs, respectively. In addition to execution time represented in Table 3.4, these three methods have been quantitatively compared based on various criteria, including overshoot, settling time, and rise time, as shown in Table 3.5.

Table 3.5 . Quantitative comparison analysis

Attack	Criterion / Method	Overshoot	Settling time	Rise time
Constant attack	**Cecilia et al. [2]**	5.6 %	0.0108 s	8.1 ms
$a_{12} = 8$	**Freidovich et al. [3]**	27.77 %	0.0926 s	15.7 ms
at $t = 3$ s	**This work**	4.4 %	0.0062 s	1.3 ms
Constant attack	**Cecilia et al. [2]**	4.85 %	0.0208 s	8.9 ms
$a_{14} = 12$	**Freidovich et al. [3]**	23.78 %	0.1584 s	17.7 ms
at $t = 4$ s	**This work**	0 %	0.0051 s	2.4 ms

3.4.10 Comparative study

In this section, a comparative study is conducted to show the superiority of the proposed method over other existing tools from the literature. For this purpose, some quality features are first defined, and then it is checked whether the proposed method has those specific features compared to other methods or not. Table 3.6 summarizes this comparative study.

Table 3.6 . Comparing the proposed method to others

Features \ methods	[2]	[49]	[88, 89]	[177]	Prop.
Parameter uncertainty	×	✓	✓	×	✓
Scalability	✓	✓	✓	✓	✓
Reliability	×	✓	✓	×	✓
Attack mitigation	✓	×	×	×	✓
Noise measurements	✓	×	✓	✓	✓
Real-time test or practicality	✓	×	×	×	✓

According to this comparison table, [49, 88, 89], and [177] are able to detect cyber-attacks. However, they do not consider attack mitigation, which is of great importance. Additionally, the performance of our proposed method against parameter uncertainties, load and attack value changes has been evaluated by real-time tests, unlike the methods mentioned above. Regarding the reliability features, contrary to [2], where an open loop observer is utilised for power lines current estimation, our proposed methodology used a robust estimator based on unknown input observers.

In the next section, the problem of cybersecurity will be considered with an other method. The most important feature of next scheme, which distinguishes it from this method, is that there is no need for a secure channel or additional information transfer in that method.

3.5 Summary

This chapter proposed a novel SM-based UIO approach for FDIA detection and its impact mitigation in dc MGs. For this purpose, each DG is equipped with a bank of SM-based UIOs for state estimation of its neighboring units. In this strategy, the equations of each DG are augmented with the attack signals. By equipping each DG with the proposed observer-based attack detection, the FDIAs in the communication links are reconstructed. Then, the detected compromised signals are

used to clean the polluted ones. To achieve the desired objectives in dc MGs (i.e., proportional current sharing and precise voltage regulation), a distributed secondary control strategy is implemented, complemented by two PI controllers at the primary control level. The secondary controller calculates the reference voltage value for each DG. In addition to providing the stability of the proposed scheme with mathematical proof, its applicability and efficiency in providing safe operation of dc MGs against different types of attacks has been demonstrated by real-time OPAL-RT results.

Chapter 4

Cyberattack Reconstruction and Mitigation with a Distributed Projection Operator-based Unknown Input Observer for DC Microgrids

As previously discussed, the primary objectives of dc MG control are to ensure secure operation through precise voltage regulation and proportional current sharing among DGs. However, these objectives can be undermined by cyber-attacks. Therefore, the development of resilient and effective strategies to ensure the secure operation of such systems is of critical importance for both academic research and industrial applications. To address the limitations of the technique introduced in Chapter 3—namely, the need to know the upper bound of unknown inputs and the reliance on transmitting one signal through a secure channel—we have developed an enhanced approach, detailed in this chapter.

In this chapter, a distributed projection operator (PO)-based UIO is developed to detect and mitigate the destructive effects of FDIAs in the communication links by cleaning the compromised signals. A key limitation in prior studies has been the absence of an integrated, distributed framework for reconstructing and mitigating the impact of FDIAs on dc MGs. To bridge this gap, this work introduces an innovative distributed PO-based UIO that restores and neutralizes the harmful effects of FDIAs by purifying corrupted communication signals. Additionally, this approach enables state estimation of neighboring DGs, aiding in the implementation of effective corrective measures. The principal contributions of this research are summarized as follows:

1. A novel set of reduced-order PO-based UIOs has been proposed to reconstruct cyber-attacks in interconnected power and information networks in a dc MG. This approach estimates the states of neighboring DGs without needing additional data exchange between DGs [49,87,91,2].

2. A unified and comprehensive detection and mitigation strategy has been designed for dc MGs with vulnerable information networks, enhancing their resilience and security against FDIAs.

This scheme's effectiveness has been tested under different cyber-attack scenarios, including both constant and dynamic FDIAs, by using real-time detection and corrective measures at the control center.

4.1 Problem formulation: DC MG modeling

In this section, the continuous-time dynamic model of a dc MG, depicted in Fig. 3.1 and represented in (3.1), is reconsidered. To develop the proposed PO-based UIO technique, the dynamic equations of the dc MG can be represented in the continuous-time state-space form as follows:

$$\begin{aligned} \dot{x}_j(t) &= A_{c_{jj}} x_j(t) + \sum_{\kappa \in \mathcal{N}_j} A_{c_{j\kappa}} x_\kappa(t) + B_{c_j} u_j(t) + M_{c_j} f_j(t), \\ y_j(t) &= C_{c_j} x_j(t), \end{aligned} \tag{4.1}$$

where $x_j(t) = [v_{dc_j}\ i_{dc_j}]^T \in \mathbb{R}^n$ and $y_j(t) \in \mathbb{R}^p$ are the system state and system measurement of the j-th DG, with the dimensions of n and p, respectively. Moreover, $f_j(t) = i_{l_j} \in \mathbb{R}$ is the exogenous input, and $u_j(t) \in \mathbb{R}^m$ denotes the primary control input. In this equation, $A_{c_{jj}} \in \mathbb{R}^{n\times n}$, $B_{c_j} \in \mathbb{R}^{n\times m}$, and $C_{c_j} \in \mathbb{R}^{p\times n}$ represent the system, the input, and the output matrices, respectively. In addition, $A_{c_{j\kappa}} \in \mathbb{R}^{n\times n}$ and $M_{c_j} \in \mathbb{R}^{n\times 1}$ are matrices that model the physical effects of neighboring DGs and local load conditions, respectively. One of the main differences of the current approach over the previous ones is the release of *Assumption* 3.1. In other words, instead of *Assumption* 3.1, the following remark is enough to develop the proposed technique.

Remark 4.1. *Each DG unit lacks information about the local load parameters, denoted as $M_{c_j} f_j(t)$, as well as the coupling dynamics of neighboring DG units, represented by $\sum_{\kappa\in\mathcal{N}_j} Ac_{j\kappa} x_\kappa(t)$. For instance, consider DG_j and DG_κ as adjacent units. In this scenario, the observer $PO_{j,\kappa}$, which is located in DG_κ to estimate the states of DG_j, treat $d_j(t) = \left(\sum_{i\in\mathcal{N}_j} \frac{v_{dc_i}}{r_{i,j}} - i_{l_j}\right)$ as an unknown input.*

By considering the new variable introduced in *Remark* 4.1 [i.e., $E_{c_j} d_j(t) = \sum_{\kappa\in\mathcal{N}_j} A_{c_{j\kappa}} x_\kappa(t) + M_{c_j} f_j(t)$], the continuous-time dynamic model of each DG can be expressed as follows:

$$\begin{aligned} \dot{x}_j(t) &= A_{c_{jj}} x_j(t) + B_{c_j} u_j(t) + E_{c_j} d_j(t), \\ y_j(t) &= C_{c_j} x_j(t), \end{aligned} \tag{4.2}$$

where

$$A_{c_{jj}} = \begin{bmatrix} -\sum_{\kappa\in\mathcal{N}_j} \frac{1}{c_{f_j} r_{j,\kappa}} & \frac{1}{c_{f_j}} \\ -\frac{1}{l_{f_j}} & -\frac{r_{f_j}}{l_{f_j}} \end{bmatrix}, B_{c_j} = \begin{bmatrix} 0 \\ \frac{1}{l_{f_j}} \end{bmatrix}, E_{c_j} = \begin{bmatrix} \frac{1}{c_{f_j}} \\ 0 \end{bmatrix}, C_{c_j} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{4.3}$$

Here, $E_{c_j} \in \mathbb{R}^{n\times q}$, where q denotes the dimension of the exogenous inputs. It should be noted that E_{c_j} is a full-column rank. Please refer to *Remark* 3.3.

In the next section, the control systems, including the primary and secondary controllers, are developed to secure the stability of the considered dc MG and its objective achievement.

4.2 Control system design

This section focuses on the design of control systems aimed at stabilizing the examined dc MG, achieving precise voltage regulation and proportional current distribution. This control system consists of two main sub-systems: i.e., primary and secondary control systems. To ensure overall stability across DG units, a primary controller is used. For this purpose, a state-feedback control system with an integral action is designed to achieve MG's objectives. Nonetheless, this primary controller cannot accomplish the desired objectives by itself . Therefore, a consensus-based distributed secondary control system is introduced to fulfill the operational goals of the dc MG. It should be noted that Assumption 3.3. holds true. In what follows, these two control systems are discussed.

4.2.1 Primary control system

In order to stabilize the voltage of all DGs, a primary controller based on the state-feedback controller with integral action is developed. For this purpose, it is required to augment the dynamic equations of each DG with the integrator action to guarantee the reference voltage tracking. To this end, the integrator's dynamic is given as follows:

$$\dot{\xi}_j(t) = v_{dc_j}^{ref}(t) - G_j y_j(t), \tag{4.4}$$

where $G_j = [1\ 0]$ and $\xi_j(t)$ denotes the integrator state internal to the controller, used for reference voltage tracking. Moreover, $v_{dc_j}^{ref}(t)$ is the reference voltage for the j-th DG, calculated by the secondary control system. Now, by using (4.4), (4.2) is augmented as follows:

$$\begin{aligned} \dot{\chi}_j(t) &= \breve{A}_{c_{jj}}\chi_j(t) + \breve{B}_{c_j}u_j(t) + \breve{E}_{c_j}d'_j(t), \\ h_j(t) &= \breve{C}_{c_j}\chi_j(t), \end{aligned} \tag{4.5}$$

where $\chi_j(t) = [x_j^T(t) \quad \xi_j(t)]^T$, $d'_j(t) = \left[d_j(t) \;\; v_{dc_j}^{ref}\right]^T$, and $h_j(t) = [v_{dc_j} \;\; i_{dc_j} \;\; \xi_j]^T$ denotes the augmented state, the augmented unknown input, and the augmented output, respectively. Here, $\breve{A}_{c_{jj}} \in \mathbb{R}^{(n+1)\times(n+1)}$, $\breve{B}_{c_j} \in \mathbb{R}^{(n+1)\times m}$, $\breve{E}_{c_j} \in \mathbb{R}^{(n+1)\times(q+1)}$, and $\breve{C}_{c_j} \in \mathbb{R}^{(p+1)\times(n+1)}$ represent the augmented matrices and vectors with appropriate size [178]. Thus, we have:

$$\breve{A}_{c_{jj}} = \begin{bmatrix} -\sum_{\kappa\in\mathcal{N}_j} \frac{1}{c_{f_j} r_{j,\kappa}} & \frac{1}{c_{f_j}} & 0 \\ -\frac{1}{l_{f_j}} & -\frac{r_{f_j}}{l_{f_j}} & 0 \\ -1 & 0 & 0 \end{bmatrix}, \breve{B}_{c_j} = \begin{bmatrix} 0 \\ \frac{1}{l_{f_j}} \\ 0 \end{bmatrix}, \breve{E}_{c_j} = \begin{bmatrix} \frac{1}{c_{f_j}} & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, \breve{C}_{c_j} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{4.6}$$

The continuous-time augmented dynamic model expressed in (4.5) can be discretized using the backward Euler approximation method. Thus, the discrete state-space dynamic model is formed:

$$\begin{aligned} \chi_j(k+1) &= \breve{A}_{jj}\chi_j(k) + \breve{B}_j u_j(k) + \breve{E}_j d'_j(k), \\ h_j(k) &= \breve{C}_j \chi_j(k), \end{aligned} \tag{4.7}$$

where $\breve{A}_{jj}$, $\breve{B}_j$, $\breve{E}_j$, and $\breve{C}_j$ are the state dynamic, the input, the exogenous input, and the output matrices after discretization, which are considered to be known with some uncertainty.

After augmenting the dynamic equations of each DG with the integral action, each of them are equipped with the following state-feedback controller [178].

$$u_j(k) = -K_j \chi_j(k), \tag{4.8}$$

where $K_j \in \mathbb{R}^{m\times(n+1)}$ is obtained with the pole-placement method, so that the matrix $(\breve{A}_{jj} - \breve{B}_j K_j)$ is Hurwitz. It is obvious that, together with the integral action, this controller defines a multi-variable proportional-integral (PI) regulator [179]. Figure 4.1 shows the root locus diagram of the system with the designed state-feedback controller with integral action. Based on this analysis, it is confirmed that the stability of the proposed control system is ensured. Note that placing the observer poles very far to the left can enhance the rejection of unknown inputs and enable rapid state estimation, which is particularly valuable in control and cybersecurity applications. However, excessively fast poles may increase sensitivity to measurement noise and lead to numerical stiffness. Therefore, the optimal pole placement is typically a compromise—fast enough to outperform system and disturbance dynamics, but not so fast that numerical issues or noise become dominant. The architecture of this

state-feedback controller with integral action is decentralized, since the computation of $u_j(k)$ requires only the states of j-th DG. Figure 4.2 illustrates the structure of this primary control system.

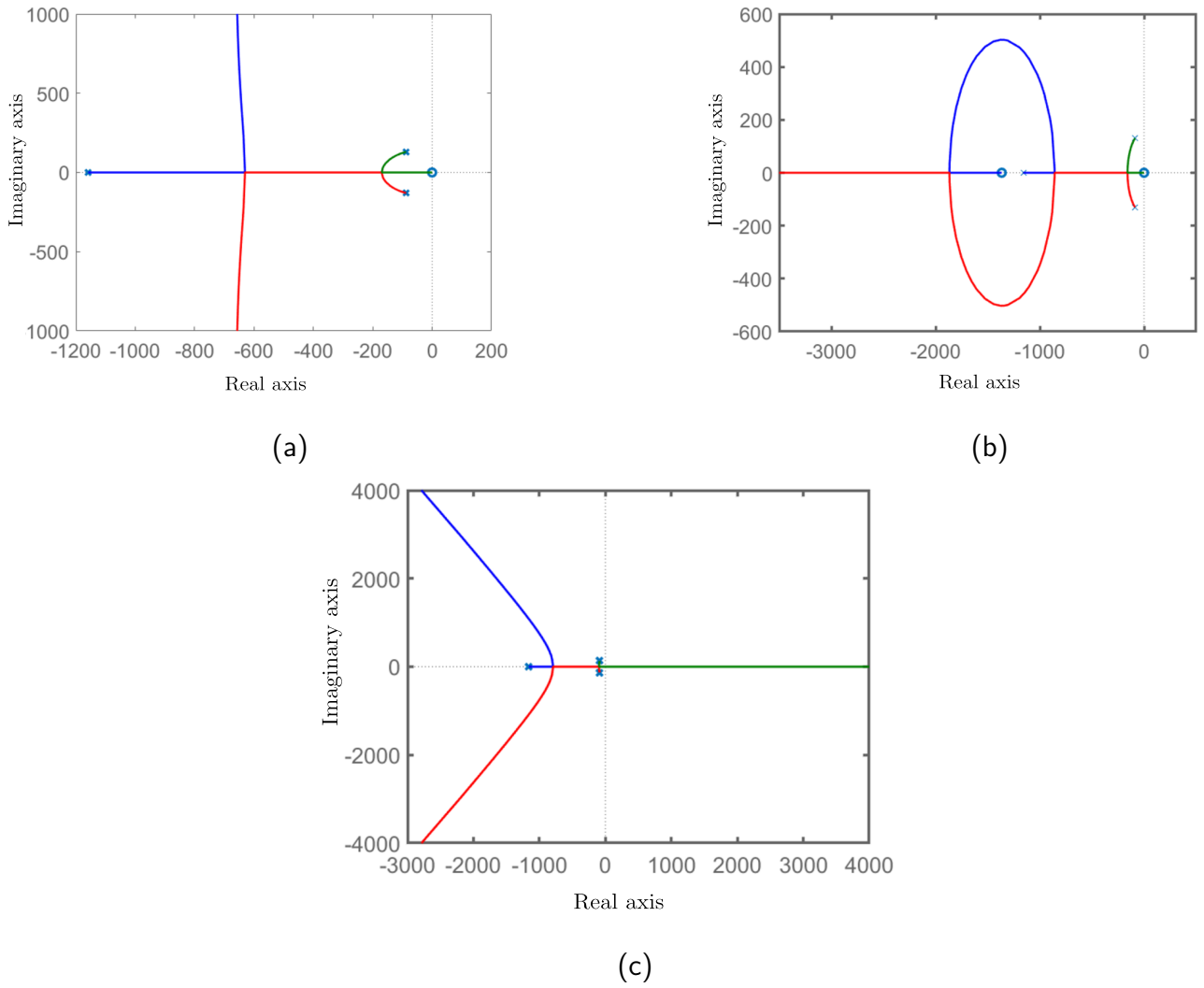


Figure 4.1 . Stability analysis of the proposed model based on the Root-Locus theory for **(a).** voltage, **(b).** current, and **(c).** integrator state.

The designed primary controller is complemented by a secondary control system, which is discussed further in the next section. This high-level control system gives each DG the reference voltage value to guarantee precise voltage regulation and proportional current sharing among all DGs.

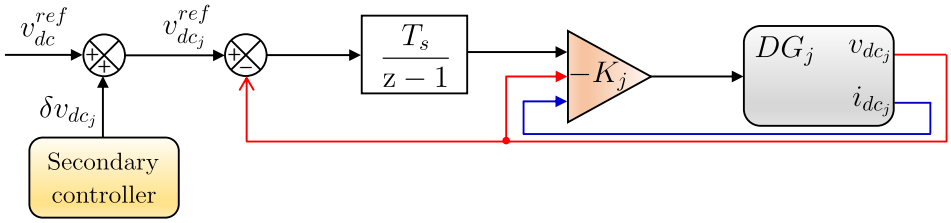


Figure 4.2 . The structure of the designed primary control system.

4.2.2 Secondary control system

This section presents a distributed secondary controller utilizing a consensus algorithm. The consensus method is widely recognized as an effective distributed technique to achieve global information sharing. Given the distributed nature of the secondary control framework, each DG unit in the network is required to communicate solely with its neighbors, regardless of the system topology. Thanks to *Definition* 3.1, to ensure a proper current distribution and maintain voltage equilibrium between DGs, the secondary controller must compute a voltage adjustment term for each DG as follows [173].

$$\delta v_{dc_j}(k+1) = \delta v_{dc_j}(k) - k_I T_s \sum_{\kappa \in \mathcal{N}_j} a_{j\kappa} \left(\frac{i_{dc_j}(k)}{i_{dc_j}^{\alpha}} - \frac{i_{dc_\kappa}(k)}{i_{dc_\kappa}^{\alpha}} \right), \tag{4.9}$$

where $a_{j\kappa} > 0$. In this equation, T_s is the sampling time. This secondary control strategy relies on neighboring DGs communicating exclusively via current signals, which makes the system vulnerable to cyber-attacks targeting this specific communication channel. However, the proposed method can be adapted to monitor and secure voltage channels, extending its applicability to broader scenarios. Once the adjustment term for each DG unit is calculated, the corresponding reference voltage for each DG can then be determined as follows:

$$v_{dc_j}^{ref}(k) = v_{dc}^{ref} + \delta v_{dc_j}(k). \tag{4.10}$$

Figure 4.3 presents the layout of the secondary control technique. In this diagram, the black block represents the communication network that connects all DGs, while the yellow block highlights the applied secondary controller as derived in (4.9). The reference voltage for each DG unit is determined by adding the computed adjustment term [i.e., $\delta v_{dc_j}(k)$] to the overall MG reference voltage. Additional details on this consensus-based secondary control approach are discussed in [173].

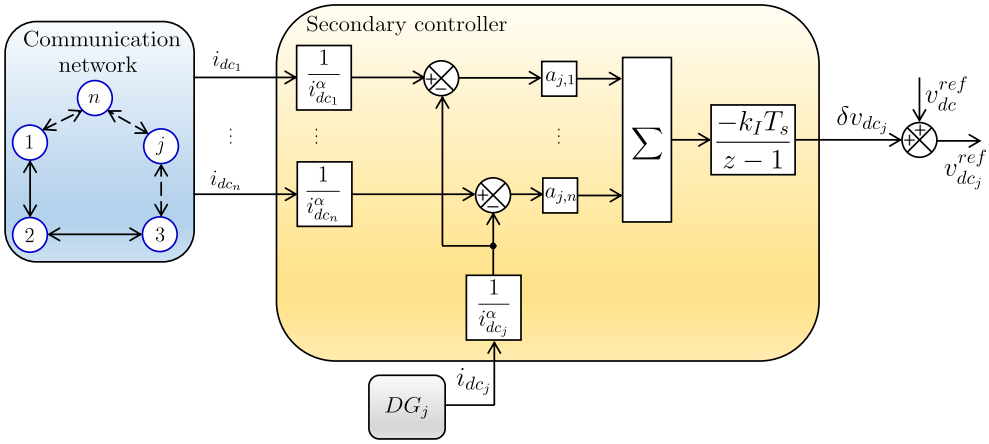


Figure 4.3 . Consensus-based secondary control structure

In the absence of FDIAs, the designed primary and secondary controllers can provide the following objectives in dc MGs [174].

$$\begin{aligned} & v^{ref}_{dc_j} = \langle \boldsymbol{v}^{ref}_{dc} \rangle, \\ & \frac{i_{dc_j}(k)}{i^{\alpha}_{dc_j}} = \frac{i_{dc_\kappa}(k)}{i^{\alpha}_{dc_\kappa}} \quad \text{for all } j, \kappa \in \mathcal{V}, \end{aligned} \tag{4.11}$$

where $\langle \boldsymbol{v}^{ref}_{dc} \rangle$ is defined in *Assumption* 3.3. The next section is dedicated to developing a PO-based UIO for detecting cyber-attacks.

4.3 PO-based UIO design

This section presents a set of PO-based reduced-order observers, developed to estimate the state variables of neighboring units in order to reconstruct possible FDIAs. These observers, deployed across all DGs, enable the estimation of neighboring DGs' states. Consequently, any cyber-attacks targeting the communication links can be identified and reconstructed within a limited time-frame. It is considered that the cyber-attacks specifically target sensor channels, and the general formulation is presented as follows:

$$\tilde{h}_j(k) = h_j(k) + \breve{D}_j a_j(k), \tag{4.12}$$

where $\tilde{h}_j(k)$ represents the compromised output signals and $\breve{D}_j \in \mathbb{R}^{(p+1)\times 1}$ denotes the attack matrices. Additionally, $a_j(k) \in \mathbb{R}$ refers to the signals associated with FDIA, which aim to disrupt data

integrity by modifying the transmitted signals with false information.

Definition 4.1. *In linear algebra and functional analysis, a projection on a vector space V is a linear operator $P : V \to V$ such that $P^2 = P$ [180].*

Similar to Section 3.2, to reconstruct attack signals using the suggested approach, the dynamic model of each DG unit is augmented in the state-space form as follows:

$$\begin{aligned} z_j(k+1) &= \bar{A}_{jj} z_j(k) + \bar{B}_j u_j(k) + \bar{E}_j d'_j(k), \\ \tilde{h}_j(k) &= \bar{C}_j z_j(k), \end{aligned} \tag{4.13}$$

where $z_j = [\chi_j^T \ a_j]^T$ denotes the augmented state, and a_j is assumed as a constant attack signal. Here $\bar{A}_{jj} \in \mathbb{R}^{(n+2)\times(n+2)}$, $\bar{B}_j \in \mathbb{R}^{(n+2)\times m}$, $\bar{E}_j \in \mathbb{R}^{(n+2)\times(q+1)}$, and $\bar{C}_j \in \mathbb{R}^{(p+1)\times(n+2)}$ denote the augmented matrices and vectors with appropriate size, where it is assumed that $(n+2) > (q+1)$. The augmented matrices are defined as follows:

$$\bar{A}_{jj} = \left[\begin{array}{c|c} \breve{A}_{jj} & \mathbf{0}_{(n+1)\times 1} \\ \hline \mathbf{0}_{1\times(n+1)} & 1 \end{array}\right], \bar{B}_j = \left[\begin{array}{c} \breve{B}_j \\ \hline 0 \end{array}\right], \bar{E}_j = \left[\begin{array}{c} \breve{E}_j \\ \hline 0 \end{array}\right], \ \bar{C}_j = \left[\begin{array}{c|c} \breve{C}_j & \breve{D}_j \end{array}\right]. \tag{4.14}$$

4.3.1 Proposed full-order PO-based attack detection

By incorporating (4.8) into (4.13), the governing equations of each DG in the discrete state-space form can be represented as:

$$\begin{aligned} z_j(k+1) &= \bar{A}_{\bar{K}_j} z_j(k) + \bar{E}_j d'_j(k), \\ \tilde{h}_j(k) &= \bar{C}_j z_j(k). \end{aligned} \tag{4.15}$$

In the above equation, $\bar{A}_{\bar{K}_j} = \bar{A}_{jj} - \bar{B}_j \bar{K}_j$, where $\bar{K}_j = [K_j, 0] \in \mathbb{R}^{m\times(n+2)}$. It's worth noting that the first element of the state-feedback control gain $\bar{K}_j$ controls the first state of the augmented system (i.e., χ_j), while the last element, which is zero, pertains to the last state of the augmented system, which is the constant attack signal. Recall that, thanks to *Remark* 4.1, it is assumed that all exogenous inputs in DG j [i.e., $\bar{E}_j d'_j(k)$] are unknown to its neighboring DGs, where $\bar{E}_j$ is a full column rank matrix. Considering $\tilde{h}_j(k)$ is measurable, the states of each DG can be decomposed as follows:

$$z_j(k) = (I_{(n+2)} - N_j \bar{C}_j) z_j(k) + N_j \bar{C}_j z_j(k) = (I_{(n+2)} - N_j \bar{C}_j) z_j(k) + N_j \tilde{h}_j(k), \tag{4.16}$$

where $N_j \in \mathbb{R}^{(n+2)\times(p+1)}$ will be specified later. In the above equation, $z_j(k)$ is decomposed into two parts, that is, the known [i.e., $N_j\tilde{h}_j(k)$] and the unknown [i.e., $\zeta_j(k) = (I_{(n+2)} - N_j\bar{C}_j)z_j(k)$] parts. It can be shown that with a proper N_j, the dynamics of the unknown parts depend only on the known quantities. For this purpose, we consider $\zeta_j(k+1)$ as:

$$\begin{aligned}\zeta_j(k+1) =&(I_{(n+2)} - N_j\bar{C}_j)z_j(k+1) = (I_{(n+2)} - N_j\bar{C}_j)\left(\bar{A}_{\bar{K}_j}z_j(k) + \bar{E}_j d'_j(k)\right)\\ =&(I_{(n+2)} - N_j\bar{C}_j)\bar{A}_{\bar{K}_j}\left(\zeta_j(k) + N_j\tilde{h}_j(k)\right) + (I_{(n+2)} - N_j\bar{C}_j)\bar{E}_j d'_j(k).\end{aligned} \tag{4.17}$$

According to (4.17), it is clear that if we choose N_j such that

$$(I_{(n+1)} - N_j\bar{C}_j)\bar{E}_j = 0, \tag{4.18}$$

then the dynamic of ζ_j depends only on the known quantity, i.e., $\tilde{h}_j$. To estimate the states of the considered dc MG [i.e., $z_j(k)$], it is required to precisely estimate $\zeta_j(k)$. Thus, we have;

$$\hat{\zeta}_j(k+1) =(I_{(n+2)} - N_j\bar{C}_j)\left(\bar{A}_{\bar{K}_j}\left(\hat{\zeta}_j(k) + N_j\tilde{h}_j(k)\right) + L_j\bar{C}_j\left(z_j(k) - \hat{z}_j(k)\right)\right), \tag{4.19}$$

where $\hat{z}_j(k)$ is assumed as an estimation of $z_j(k)$, and $L_j \in \mathbb{R}^{(n+2)\times(p+1)}$ is the observer gain that will be designed later. Let $e_j(k) = z_j(k) - \hat{z}_j(k)$. In *Theorem* 4.1, it will be shown that with the proposed PO-based UIO, $e_j(k) \to 0$ as $t \to \infty$. To proceed further, we need the following conditions and lemma.

Condition 4.1. $\operatorname{rank}\left(\bar{C}_j\bar{E}_j\right) = \operatorname{rank}\bar{E}_j$, *which indicates that this technique is applicable when the number of unknown inputs is less than the number of outputs.*

Condition 4.2. $\operatorname{rank}\begin{bmatrix} \mathrm{z}I_{(n+2)} - \bar{A}_{\bar{K}_j} & \bar{E}_j \\ \bar{C}_j & 0 \end{bmatrix} = n + q + 3$, *for all* $|\mathrm{z}| \geq 1$.

Lemma 4.1. *Assume that* $\check{P}_j : \mathbb{R}^{(n+2)} \to \mathbb{R}^{(n+2)}$ *is a projection, where* $\operatorname{rank}\check{P}_j = n - q + 1$. *Then,* $\check{P}_j$ *has* $(n - q + 1)$ *eigenvalues equal to* 1 *and* $(q + 1)$ *eigenvalues equal to* 0. *In addition, there is a basis of* $\mathbb{R}^{(n+2)}$, *as follows:*

$$G_j^{-1}\check{P}_j G_j = P_j = \begin{bmatrix} I_{(n-q+1)} & 0 \\ 0 & 0_{(q+1)} \end{bmatrix}, \tag{4.20}$$

where $G_j \in \mathbb{R}^{(n+2)\times(n+2)}$ *is an invertible matrix whose columns are the eigenvectors of matrix* $\check{P}_j$ *[180].*

Theorem 4.1. *Assume that Condition 4.1 and Condition 4.2 hold true, then there exists a gain matrix L_j so that the estimation error [i.e., $e_j(k)$] converges to 0 as $t \to \infty$.*

Proof: Considering the definition of error estimation [i.e., $e_j(k) = z_j(k) - \hat{z}_j(k)$] and using $\hat{z}_j(k) = \hat{\zeta}_j(k) + N_j h_j(k)$, (4.15), and (4.19), the first forward difference of dynamic estimation error can be represented as follows:

$$\begin{aligned} e_j(k+1) &= z_j(k+1) - \hat{z}_j(k+1) \\ &= z_j(k+1) - \hat{\zeta}_j(k+1) - N_j\bar{C}_j z_j(k+1) = \left(I_{(n+2)} - N_j\bar{C}_j\right) z_j(k+1) - \hat{\zeta}_j(k+1) \\ &= \left(I_{(n+2)} - N_j\bar{C}_j\right)\left(\left(\bar{A}_{\bar{K}_j} z_j(k) + \bar{E}_j d'_j(k)\right) - \bar{A}_{\bar{K}_j}\left(\hat{\zeta}_j(k) + N_j\tilde{h}_j(k)\right) - \left(L_j\bar{C}_j(z_j(k) - \hat{z}_j(k))\right)\right). \end{aligned} \tag{4.21}$$

Thanks to (4.18), (4.21) can be simplified as follows:

$$\begin{aligned} e_j(k+1) &= \left(I_{(n+2)} - N_j\bar{C}_j\right)\left(\bar{A}_{\bar{K}_j}\left(z_j(k) - \hat{z}_j(k)\right) - L_j\bar{C}_j\left(z_j(k) - \hat{z}_j(k)\right)\right) \\ &= \left(I_{(n+2)} - N_j\bar{C}_j\right)\left(\bar{A}_{\bar{K}_j} - L_j\bar{C}_j\right) e_j(k). \end{aligned} \tag{4.22}$$

Now, we will specify the proper N_j and L_j such that $e_j(k) \to 0$ for $t \to \infty$.

To derive the dynamic estimation error, it is assumed that (4.18) holds. A solution to this equation under *Condition* 4.1 is given by [181]:

$$N_j = \bar{E}_j\left(\bar{C}_j\bar{E}_j\right)^{\dagger}, \tag{4.23}$$

where the superscript † is the Moore-Penrose pseudo-inverse operation. It should be noted that (4.23) can be simplified to $N_j = \bar{E}_j(\bar{C}_j\bar{E}_j)^{-1}$ when $\bar{C}_j\bar{E}_j$ is a square matrix, and as a result, it becomes invertible [182]. Thanks to the properties of the Moore-Penrose pseudo-inverse operation (i.e., $\left(\bar{C}_j\bar{E}_j\right)^{\dagger}\left(\bar{C}_j\bar{E}_j\right)\left(\bar{C}_j\bar{E}_j\right)^{\dagger} = \left(\bar{C}_j\bar{E}_j\right)^{\dagger}$ [180]), it can be shown that $N_j\bar{C}_j$ is a projection [i.e., $(N_j\bar{C}_j)^2 = N_j\bar{C}_j$], and as a result, $\check{P}_j = I_{(n+2)} - N_j\bar{C}_j$ is also a projection [182].

Using the result of *Lemma* 4.1, the following coordinate transformation matrix is introduced:

$$\check{e}_j(k) = G_j^{-1} e_j(k). \tag{4.24}$$

Now, by applying this coordinate transformation matrix to (4.22), we obtain:

$$\check{e}_j(k+1) = P_j G_j^{-1}\left(\bar{A}_{\bar{K}_j} - L_j\bar{C}_j\right) G_j\check{e}_j(k). \tag{4.25}$$

where

$$\check{A}_{\bar{K}_j} = G_j^{-1}\bar{A}_{\bar{K}_j}G_j = \begin{bmatrix} \check{A}_{\bar{K}_{j,11}} & \check{A}_{\bar{K}_{j,12}} \\ \check{A}_{\bar{K}_{j,21}} & \check{A}_{\bar{K}_{j,22}} \end{bmatrix}, \check{L}_j \ = G_j^{-1}L_j = \begin{bmatrix} \check{L}_{j,1} \\ \check{L}_{j,2} \end{bmatrix}, \ \check{C}_j = \bar{C}_j G_j = \begin{bmatrix} \check{C}_{j,1} & \check{C}_{j,2} \end{bmatrix}, \tag{4.26}$$

where $\check{A}_{\bar{K}_{j,11}} \in \mathbb{R}^{(n-q+1)\times(n-q+1)}$, $\check{A}_{\bar{K}_{j,12}} \in \mathbb{R}^{(n-q+1)\times(q+1)}$, $\check{A}_{\bar{K}_{j,21}} \in \mathbb{R}^{(q+1)\times(n-q+1)}$, $\check{A}_{\bar{K}_{j,22}} \in \mathbb{R}^{(q+1)\times(q+1)}$, $\check{L}_{j,1} \in \mathbb{R}^{(n-q+1)\times(p+1)}$, $\check{L}_{j,2} \in \mathbb{R}^{(q+1)\times(p+1)}$, $\check{C}_{j,1} \in \mathbb{R}^{(p+1)\times(p-q)}$, and $\check{C}_{j,2} \in \mathbb{R}^{(p+1)\times(q+1)}$. Now, by substituting (4.26) into (4.25), we obtain:

$$\check{e}_j(k+1) = P_j(\check{A}_j - \check{L}_j\check{C}_j)\check{e}_j(k) = \begin{bmatrix} \check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1} & \check{A}_{\bar{K}_{j,12}} - \check{L}_{j,1}\check{C}_{j,2} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \check{e}_{j,1}(k) \\ \check{e}_{j,2}(k) \end{bmatrix}, \tag{4.27}$$

where $\check{e}_{j,1}(k) \in \mathbb{R}^{(n-q+1)}$ and $\check{e}_{j,2}(k) \in \mathbb{R}^{(q+1)}$. As is clear, $\check{e}_{j,2}(k+1) = 0$. Thus, it can be concluded that $\check{e}_{j,2}(k) = 0$ for all samples $k \geq 1$. As a result, (4.27) can be simplified as follows:

$$\check{e}_{j,1}(k+1) = \left(\check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1}\right)\check{e}_{j,1}(k). \tag{4.28}$$

Given that *Condition* 4.2 holds, the pair $\left(\check{A}_{\bar{K}_{j,11}}, \check{C}_{j,1}\right)$ defined in (4.28) is detectable [173]. Then we can find a matrix $\check{L}_{j,1}$ such that $\left(\check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1}\right)$ is Hurwitz. It is clear from (4.28) that $\check{e}_{j,1} \to 0$. According to (4.27), it can be concluded that $\check{e}_j \to 0$.

It is now required to design the observer gain (i.e., $\check{L}_{j,1}$). For this purpose, this observer gain is obtained by a Luenberger observer method, which allows locating the poles of the observer in its desired locations. Under *Conditions* 4.1 and 4.2, it can be concluded that the estimation error converges to 0 as $t \to \infty$, which completes the proof. ■

4.3.2 Reduced-order projection operator-based attack detection

As above-mentioned, when $\check{e}_{j,2}$ tends to zero for all samples $k \geq 1$, the estimation error of the system is completely dependent on $\check{e}_{j,1}$ [See (4.28)]. As a result, estimating $\check{e}_{j,2}$ is not required. Thus, let's apply the G_j^{-1} transformation, which was previously applied to $e_j(k)$ in (4.24), to $\hat{\zeta}_j(k)$, as follows:

$$\check{\zeta}_j(k) = G_j^{-1}\hat{\zeta}_j(k). \tag{4.29}$$

Now, by using (4.19) and *Lemma* 4.1, we have

$$\check{\zeta}_j(k+1) = P_j G_j^{-1}\left[\bar{A}_{\bar{K}_j}G_i\check{\zeta}_j(k) + \bar{A}_{\bar{K}_j}N_j\tilde{h}_j(k) + L_j(\tilde{h}_j(k) - \bar{C}_j\hat{\zeta}_j(k) - \bar{C}_jN_j\tilde{h}_j(k))\right]. \tag{4.30}$$

According to (4.29), $\hat{\zeta}_j(k) = G_j\check{\zeta}_j(k)$; thus,

$$\check{\zeta}_j(k+1) = P_jG_j^{-1}\left(\bar{A}_{\bar{K}_j}G_j - L_j\bar{C}_jG_j\right)\check{\zeta}_j(k) + P_jG_j^{-1}\left(\bar{A}_{\bar{K}_j}N_j + L_j - L_j\bar{C}_jN_j\right)\tilde{h}_j(k), \tag{4.31}$$

which can be simplified by (4.26), as follows:

$$\check{\zeta}_j(k+1) = P_j(\check{A}_{\bar{K}_j} - \check{L}_j\check{C}_j)\check{\zeta}_j(k) + P_jG_j^{-1}\left[\left(\bar{A}_{\bar{K}_j}N_j + G_j\check{L}_j\left(I_{(p+1)} - \bar{C}_jN_j\right)\right)\tilde{h}_j(k)\right]. \tag{4.32}$$

We can define $\check{\zeta}_j(k) = \begin{bmatrix} \check{\zeta}_{j,1}(k) \\ \check{\zeta}_{j,2}(k) \end{bmatrix}$, where $\check{\zeta}_{j,1} \in \mathbb{R}^{(n-q+1)}$ and $\check{\zeta}_{j,2} \in \mathbb{R}^{(q+1)}$. Thanks to the structure of matrix P_j [see (4.20)] and since this matrix is pre-multiplied to (4.32), we can make sure that $\check{\zeta}_{j,2}(k) = 0$ for all samples $k \geq 1$. As a result, by estimating only $(n-q+1)$ states with the observer and ignoring the remaining $(q+1)$ states, the resulting reduced-order observer can be represented as follows:

$$\begin{aligned} \check{\zeta}_{j,1}(k+1) &= \left(\check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1}\right)\check{\zeta}_{j,1}(k) + \left[I_{(n-q+1)}\ 0_{(q+1)}\right] \times G_j^{-1}\check{S}_j\tilde{h}_j(k), \\ \hat{z}_j(k) &= G_j\begin{bmatrix} I_{(n-q+1)} \\ 0_{(q+1)\times(n-q+1)} \end{bmatrix}\check{\zeta}_{j,1}(k) + N_j\tilde{h}_j(k), \end{aligned} \tag{4.33}$$

where $\check{S}_j = \bar{A}_{\bar{K}_j}N_j + G_j\check{L}_j\left(I_{(p+1)} - \bar{C}_jN_j\right)$, and $\hat{z}_j(k)$ is the state estimation. Moreover, with respect to (4.26) and since we only need to estimate $\check{\zeta}_{j,1}(k+1)$, $\check{L}_j$ can be represented as follows:

$$\check{L}_j = \begin{bmatrix} \check{L}_{j,1} \\ 0_{(q+1)\times(p+1)} \end{bmatrix}. \tag{4.34}$$

Remark 4.2. *The projection operator's key advantage lies in its ability to decouple state estimation errors from unknown inputs, enabling reduced-order estimation by focusing only on $(n-q+1)$ states and disregarding the remaining $(q+1)$ states. Additionally, the proposed PO-based UIO enhances resilience to various types of cyber-attacks by eliminating the effects of unknown inputs during state estimation, without requiring knowledge of their upper bound. This scheme offers a straightforward design process that can be easily implemented in the dc MG just by following Algorithm 4.1.*

A summary of how the PO-based attack reconstruction scheme can be implemented is provided in the following section. To ensure safe operation of the considered dc MG, it is necessary to equip each DG with a bank of PO-based UIOs. By doing so, all communication signals that may be

affected by intruders are cleaned, thereby enabling effective attack mitigation. Figure 4.4 provides an overview of the proposed PO-based UIO structure. The green section represents the dynamic model of the system, capturing both known and unknown inputs in its augmented format. Meanwhile, the yellow section illustrates the observer framework used for detecting potential attacks. Although this PO-based UIO scheme is developed for dc MGs, it can be adapted and designed for a wide range of applications, including power grids, wireless sensor networks, autonomous vehicle networks, robotics, and so on.

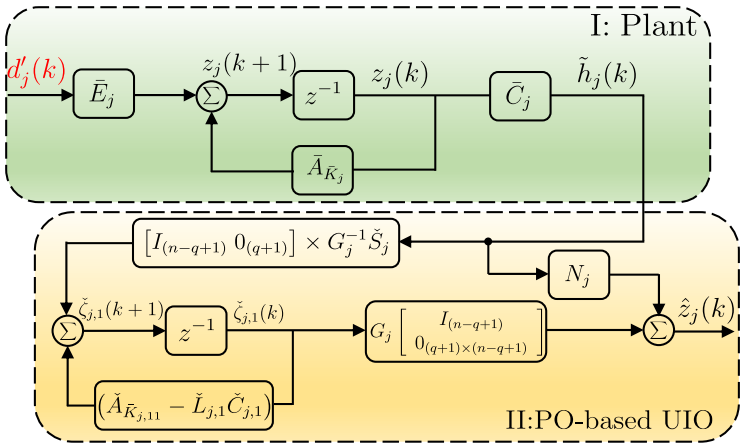


Figure 4.4 . The proposed PO-based UIO structure.

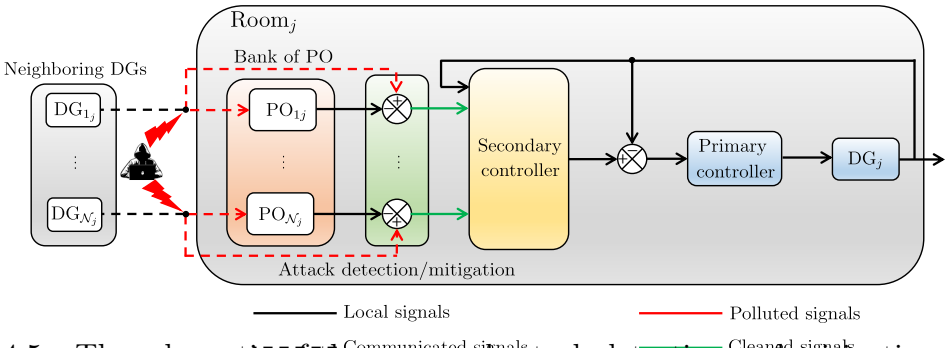


Figure 4.5 . The schematic of the proposed attack detection and mitigation scheme

Algorithm 4.1 PO-based UIO design procedure

Input: Matrices $\bar{A}_{\bar{K}_j}$, $\bar{E}_j$, $\bar{C}_j$, and signal $\tilde{h}_j(k)$.

1: **if** *Condition* 4.1 is not satisfied **then**
2: STOP
3: **else**
4: Compute N_j by (4.23).
5: Compute $\check{P}_j$, and G_j with (4.20).
6: Compute $\check{A}_{K_j}$, and $\check{C}_j$ with (4.26).
7: **if** *Condition* 4.2 is not satisfied **then**
8: STOP
9: **else**
10: Design $\check{L}_{j,1}$ so that $\left(\check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1}\right)$ is Hurwitz.
11: Form $\check{L}_j$ by (4.34).
12: Compute $\check{S}_j$.
13: Construct the PO observer by (4.33).

4.3.3 Proposed observer implementation

This section explains the implementation of the proposed PO-based UIO within an MG context. First, it is required to derive the augmented matrices of the dc MG, represented in (4.13). Then, N_j should be calculated with (4.23) to make the dynamic of unknown parts to be dependent on just known quantities. With the proper G_j calculated with (4.20), $\check{A}_{K_j}$, and $\check{C}_{j,1}$ should be obtained with (4.26). Afterwards, the matrix $(\check{A}_{\bar{K}_{j,11}} - \check{L}_{j,1}\check{C}_{j,1})$ is ensured to be Hurwitz by selecting $\check{L}_{j,1}$ through the pole-placement method. Regardless of the number of DG units, each observer is of order two due to the transformation applied. The design of the observer gain follows the standard second-order pole-placement approach. Afterward, the values of $\check{L}_j$ and $\check{S}_j$ are determined. The final design of the proposed PO-based UIO, as presented in (4.33), is then completed. It is crucial to verify that *Conditions* 4.1 and 4.2 are met prior to applying this method. A detailed overview of the PO-based state estimation and attack detection is illustrated in Fig. 4.5 and Algorithm 4.1.

4.4 Results and discussions

This section evaluates the proposed strategy under diverse scenarios, including changes in local load, dynamic FDIAs, and real-world communication testing. Real-time simulation results confirm the approach's ability to manage both limited and unlimited time-dependent FDIA cases effectively.

4.4.1 Performance evaluation of the proposed scheme

This section aims to assess the proposed scheme's effectiveness. The setup involves a four-DG dc MG configuration with interconnecting inductive/resistive lines, modeled on the OPAL-RT real-time simulator. The arrangement, which includes OPAL-RT, a host laptop, and an oscilloscope, is illustrated in Fig. 4.6(a), where the host laptop functions as an asynchronous user interface. Figure 4.6(b) displays the MG's schematic. Even-numbered DGs (DG_2 and DG_4) are assumed to have twice the capacity of the odd-numbered ones. The specific MG parameters are outlined in Table 4.1, with the selected resistances and inductances for power lines set as follows: $r_{12} = 0.36\ \Omega$, $r_{23} = 0.5\ \Omega$, $r_{34} = 0.55\ \Omega$, $r_{14} = 0.4\ \Omega$, $l_{12} = 10\ \mu$H, $l_{23} = 20\ \mu$H, $l_{34} = 25\ \mu$H, $l_{14} = 50\ \mu$H.

It is assumed reference voltage is $v_{dc}^{ref} = 320$ V. To show the effectiveness of the utilised control systems in maintaining stability, they are implemented on the dc MG without any FDIAs. As illustrated in Fig. 4.7(a), the voltage/current data for all DGs indicate the precise voltage control and

Table 4.1 . Parameters of the four-DG MG for simulations

Unit \ Symbol	r_{f_j} (Ω)	l_{f_j} $(m\text{H})$	c_{f_j} $(m\text{F})$	r_j (Ω)
DG_1	1	2.5	3.5	50
DG_2	0.75	3	5	40
DG_3	1.2	3.5	2	55
DG_4	1.1	2	4	45

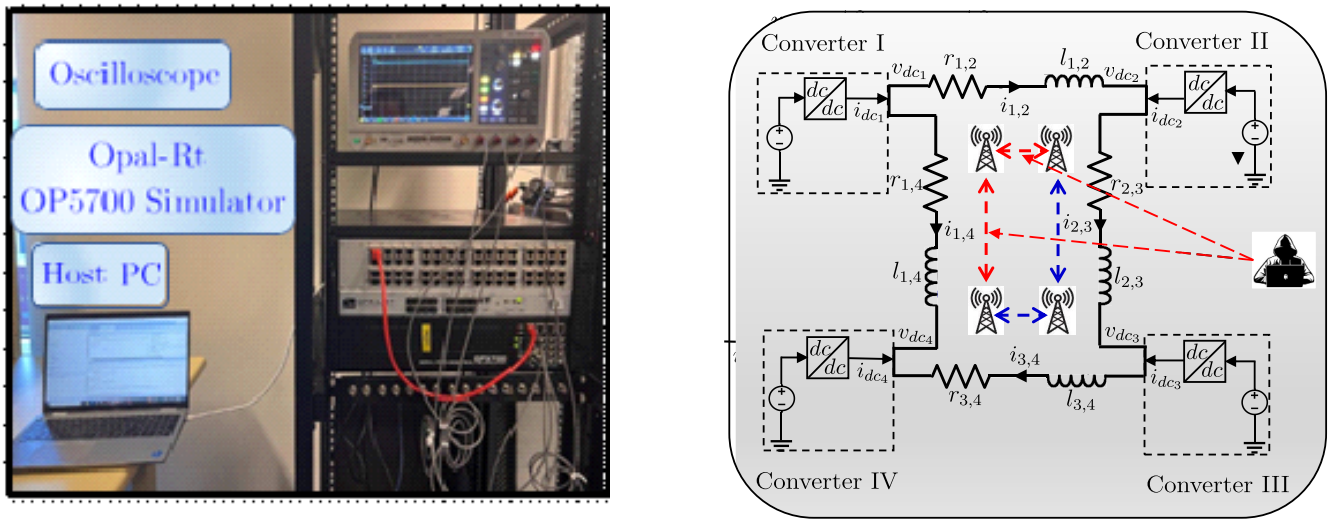


Figure 4.6 . **(a).** The real-time setup, **(b).** The under-study dc microgrid.

successful proportional current sharing. However, adverse factors such as cyber intrusions, parameter variations, and other disturbances are unavoidable. In Fig. 4.7(b), the system's voltage/current response under FDIA conditions, with no attack detection/mitigation in place, is shown. The unmet objectives, particularly (4.11), underscore the critical need for robust cybersecurity measures. This scenario includes two FDIAs targeting the communication pathways of DG_1 and adjacent units: a constant FDIA at $t = 2$ s and another at $t = 4$ s, impacting DG_2 and DG_4.

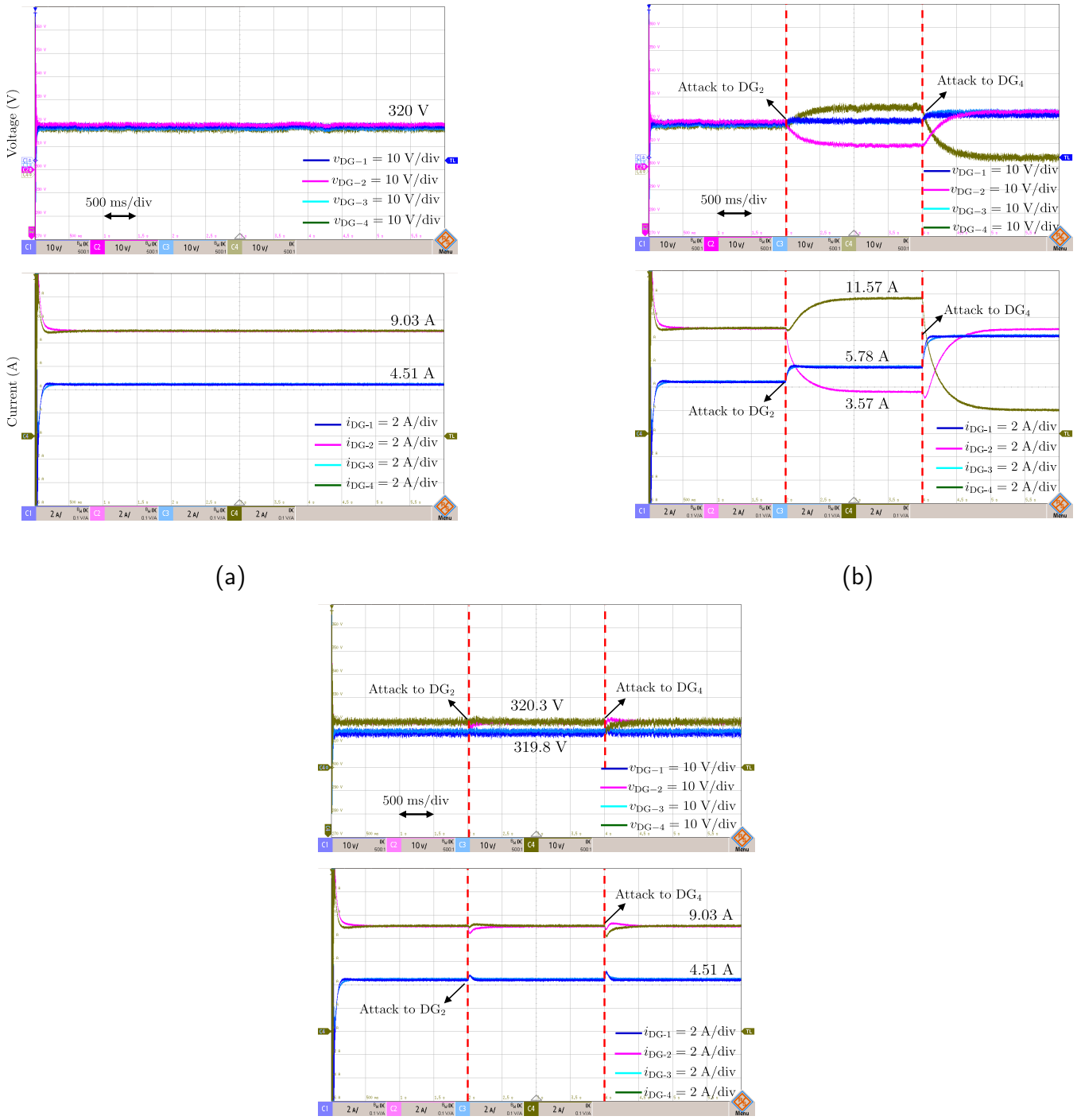


Figure 4.7 . The voltages/currents for all DGs **(a)**. under normal condition, **(b)**. for the compromised MG operating without any attack reconstruction, **(c)**. against FDIA with the proposed scheme.

After assessing the impact of FDIA on the dc MG without implementing the suggested mechanism, we later apply this strategy to detect and eliminate FDIA effects. Figure 4.8 illustrates the block diagram for implementing the proposed scheme. As shown in Fig. 4.7(c), the proposed PO-based UIO effectively detects and mitigates FDIAs, thereby satisfying (4.11). Additionally, Fig. 4.9(a) presents a comparison between actual and estimated FDIA profiles, further demonstrating the method's accuracy in identifying these attacks. The RMSE values of 0.032 and 0.028 for the respective attack estimations demonstrate the high accuracy of the proposed scheme in detecting cyber-attacks.

Figure 4.9(b) highlights the capacity of each DG.

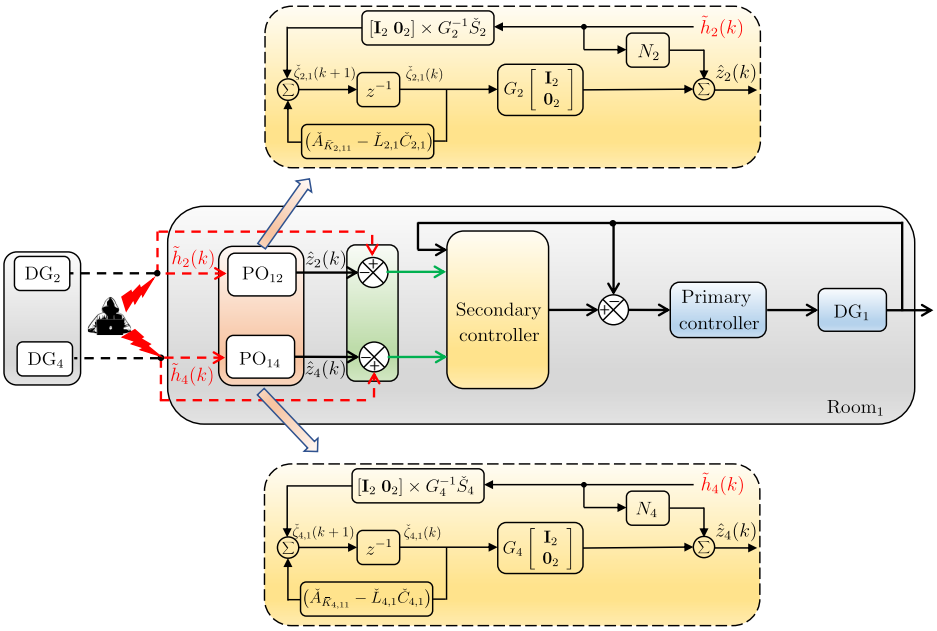
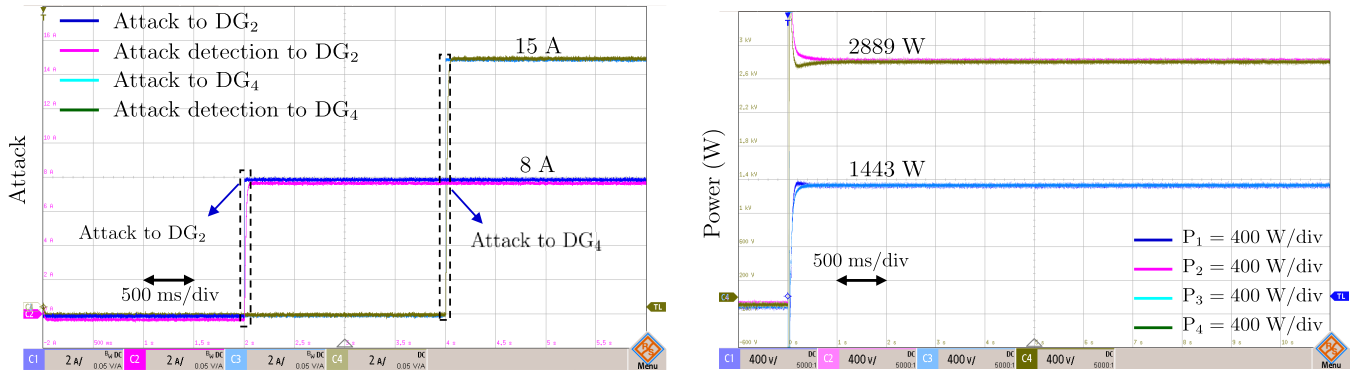


Figure 4.8 . Block diagram of case study A.

4.4.2 Performance evaluation against constant attack change and load change conditions

In this section, a new scenario is used to assess the ability of the proposed scheme to respond effectively to both planned and unplanned situations, such as variations in local loads and attack values. During network operation, local loads in each DG can fluctuate unexpectedly. The method should, therefore, reliably detect these attack events. For example, the attack on DG_2 is assumed to increase from 5 A to 8 A at $t = 3$s, while for DG_4, the FDIA value is raised from 7 A to 15 A



(a) (b)

Figure 4.9 . **(a)**. FDIA reconstruction with the proposed strategy, **(b).** Power of each DG.

at $t = 4$ s. Additionally, at $t = 5$ s, the local load of DG_4 shifts from 40 Ω to 45 Ω. As shown in Fig. 4.10(a) and (b), which illustrate current and voltage across all DGs, the approach maintains its effectiveness under these conditions. Fig. 4.10(c) further displays the actual FDIA profile alongside the estimated one.

4.4.3 Performance evaluation against unbounded time-varying cyber-attacks

Unlike noise and fault signals, which are typically bounded, attack signals can be unbounded, as they are intentionally crafted to inflict maximum damage [183]. A key advantage of the proposed method over other approaches is its capacity to handle dynamic cyber-attacks that change over time. To verify this, we tested the method specifically against time-varying cyber-attacks. Thus, two time-dependent FDIAs were introduced to the communication paths of DG_1 and its neighboring units: an unbounded time-varying FDIA with $a_{12} = 5t$ at $t = 2$ s and another, $a_{14} = 12t$, at $t = 4$s, affecting DG_2 and DG_4, respectively. Before demonstrating the method's resistance to these cyber-attacks, the effects of unbounded FDIAs on the under-study dc MG are illustrated in Fig. 4.11(a). As shown, the intended objectives of the dc MG, represented by (4.11), are unmet. Once the proposed detection scheme is activated, however, the unbounded FDIAs are effectively reconstructed. Fig. 4.11(b) confirms that (4.11) is achieved, and Fig. 4.12 displays successful detection of the time-varying FDIAs with the PO-based UIO approach.

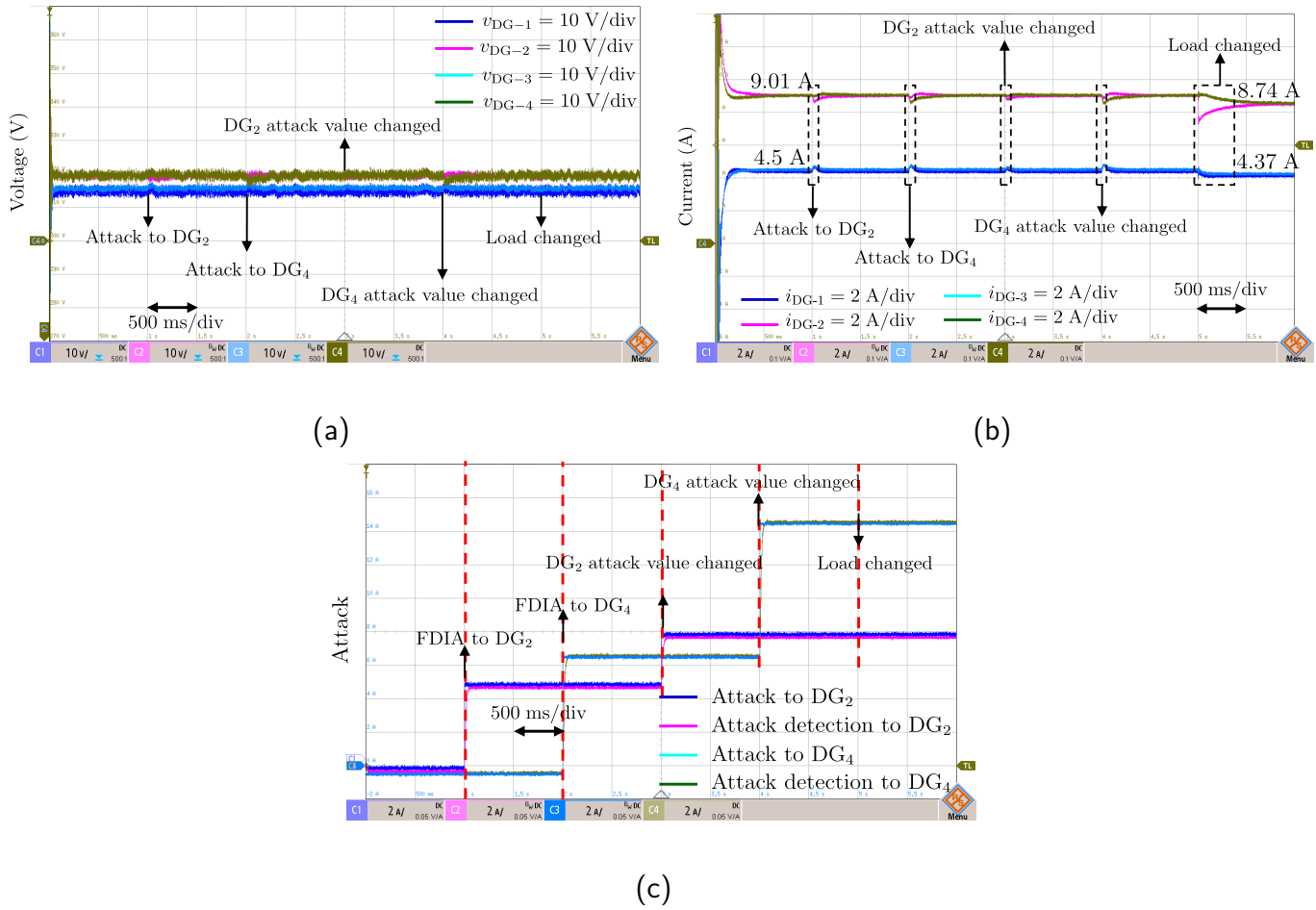
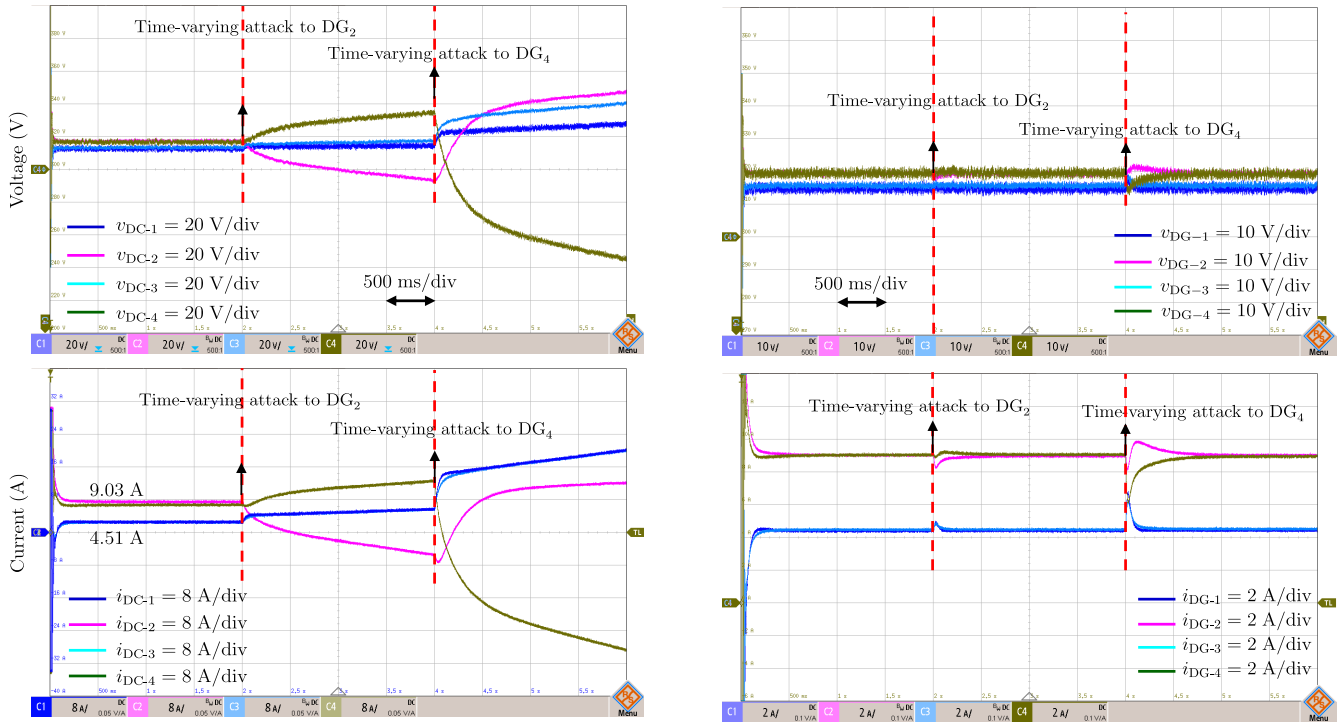


Figure 4.10 . **(a).** Voltages of all DGs, **(b).** Currents of all DGs, and **(c).** FDIA reconstruction with the suggested scheme against attack and load change conditions.

4.4.4 Performance evaluation under real communication

In this section, we evaluate the performance of our proposed PO-based UIO in a real communication scenario. To achieve this, we set up a configuration where two OPAL-RT simulators are connected via the RS-232 protocol. In this setup, DG_2 runs on the OPAL-RT 4510, while three other DGs operate on the OPAL-RT 5700. Both OPAL-RT simulators have a sampling time of 50 μs, while the communication between them is sampled every 2.5 ms, which emulates both delay and throughput restrictions in real-world applications. Figure 4.13 provides a schematic overview of this experimental setup, illustrating the connections between the simulators and communication interfaces.



(a) (b)

Figure 4.11 . Voltages/currents of the compromised MG under time-varying FDIAs operating **(a).** without any attack reconstruction scheme, **(b).** with the proposed technique.

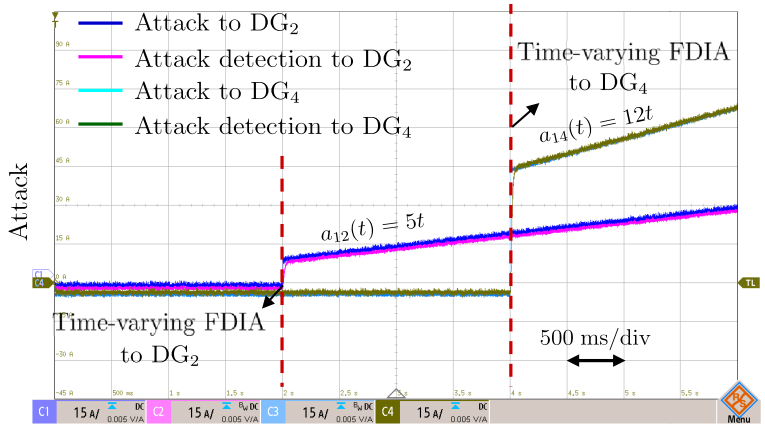


Figure 4.12 . Time-varying FDIA detection with the proposed PO-based UIO strategy

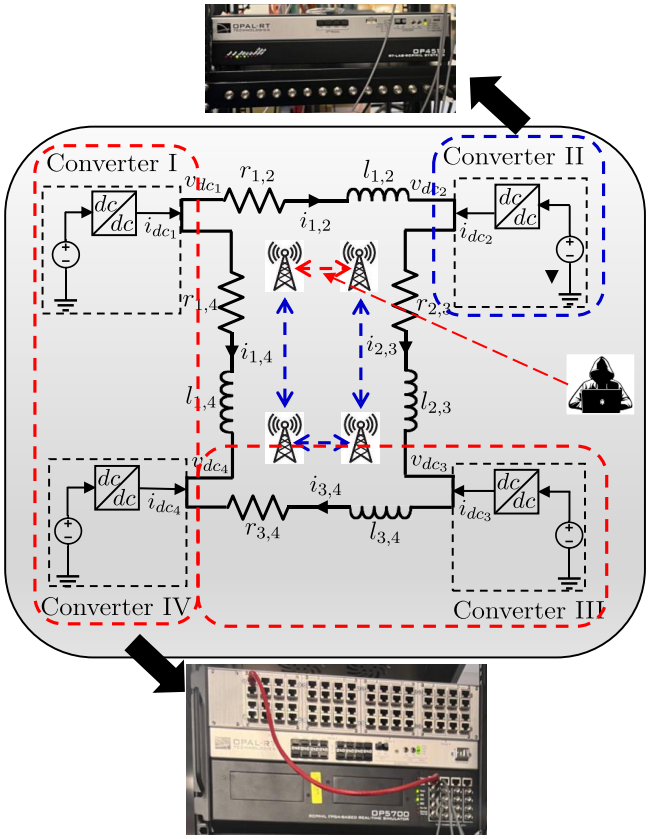


Figure 4.13 . Overview of the experimental setup.

After DG_1 receives corrupted signals from DG_2, the proposed PO-based UIO at DG_1 estimates DG_2's states, enabling reconstruction of the attack signal embedded within the received signals. As mentioned above, the main advantage of this technique is its ability to detect attack signals locally by using inputs received from neighboring units. This capability allows us to identify existing attacks in communication signals without concern for potential new attacks. Figure 4.14 confirms that our proposed scheme effectively counteracts polluted signals from neighboring units. Specifically, when DG_1 receives corrupted signals from DG_2, it reconstructs the attack signal and mitigates its harmful impact on the system. Figure 4.15 shows the actual attack signal alongside its estimated profile, reconstructed by the proposed PO-based UIO in DG_1.

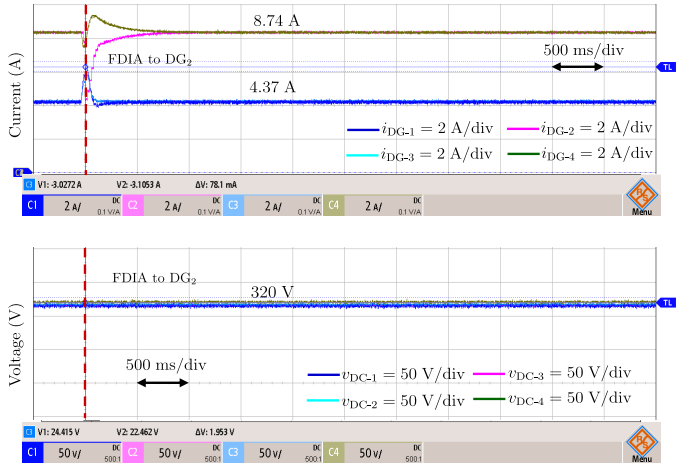


Figure 4.14 . The current and voltage profiles of all DGs under real communication test.

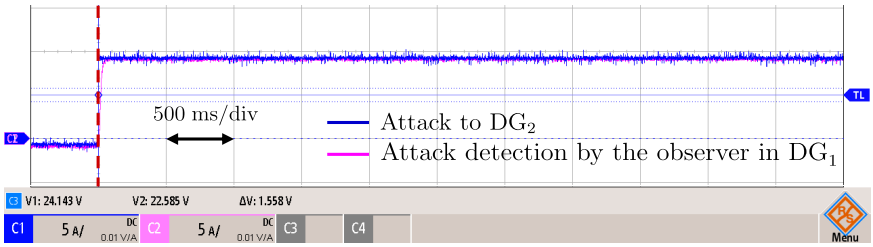


Figure 4.15 . FDIA detection with the proposed PO-based UIO strategy under real communication test.

4.4.5 Performance evaluation under fast attack signals

This section evaluates the performance of our proposed attack reconstruction and mitigation method against fast attack signals. Two bounded FDIAs were introduced into the communication paths of DG_1 and its neighboring units to assess the scheme. The first attack, a sinusoidal waveform FDIA represented as $a_{12} = 5\sin(100\pi t)$, was initiated at $t = 2$ s on the communication channel from DG_1 to DG_2. The second attack, defined $a_{14} = 8\sin(100\pi t)$, was launched at $t = 4$ s, targeting the communication channel from DG_1 to DG_4, respectively. To highlight the destructive impacts of these attacks on the studied dc MG, the system's dynamic response without the proposed mitigation scheme is presented in Fig. 4.16(a). The results show that the primary objectives of the dc MG—proportional current sharing and accurate voltage regulation—are not maintained under these attack conditions.

When the proposed PO-based UIO is applied, the mitigation scheme effectively counters the attack impacts. According to Fig. 4.16(b), it is clear that (4.11) has been satisfied. Furthermore, Fig. 4.17 demonstrates the accurate reconstruction of the attack signals and their estimated profiles, confirming the effectiveness of the mitigation strategy against fast attacks.

This study shows that the proposed scheme is capable of distinguishing anomaly occurrences, regardless of the speed at which they occur. Afterwards, the detection system can notify the operator regarding the existence of an attack in the network.

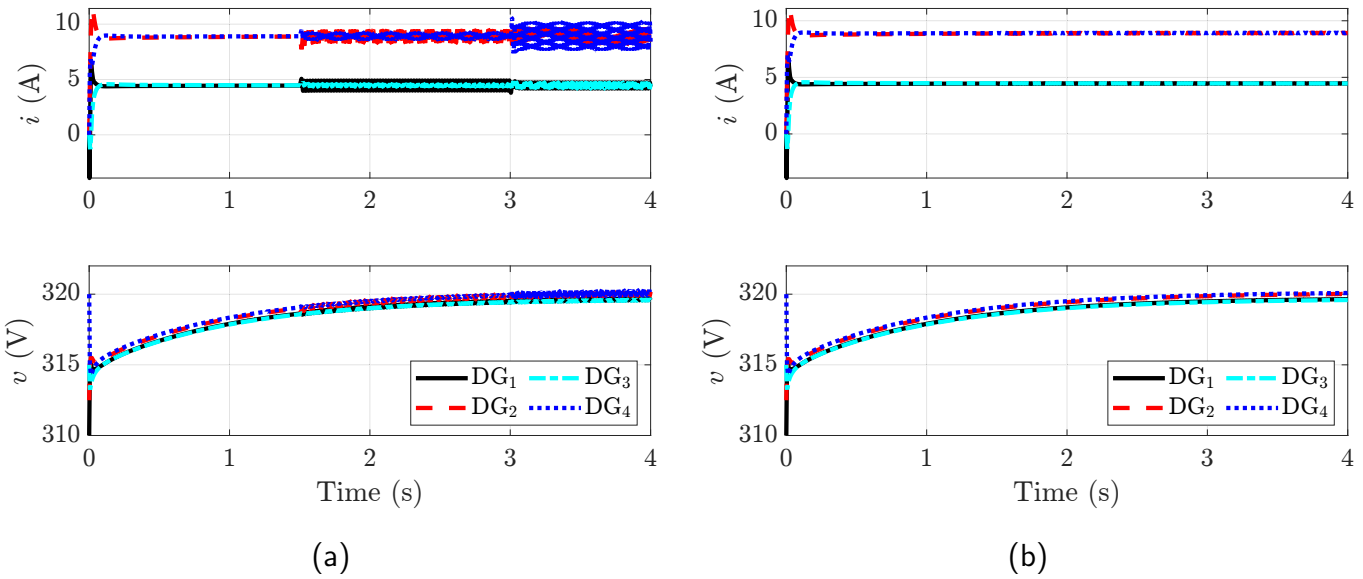


Figure 4.16 . **(a)**. The current/voltage profiles of all DGs under fast sinusoidal waveform attacks without the proposed scheme. **(b).** Performance evaluation of the proposed scheme against fast sinusoidal waveform attacks.

4.4.6 Numerical comparison

This section presents a numerical comparison between the proposed technique and those outlined in [2] and [3]. For consistency, the comparison assumes that each DG generates the same amount of power. Similarly to our approach presented in Chapter 3, this scheme requires only the exchange of current signals, reducing potential vulnerabilities to cyber threats. However, the technique proposed by [2] requires the exchange of currents and voltages between neighbors, increasing the risk of cyber-attacks on the MG.

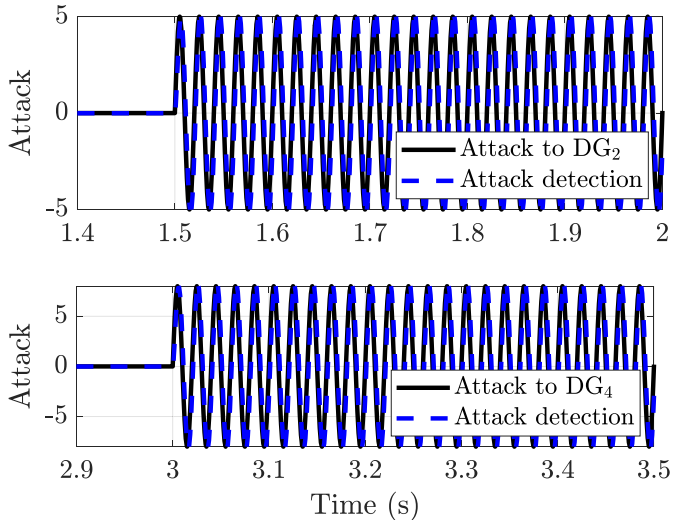


Figure 4.17 . Attack reconstruction with the proposed PO-based UIO strategy under fast sinusoidal waveform attacks.

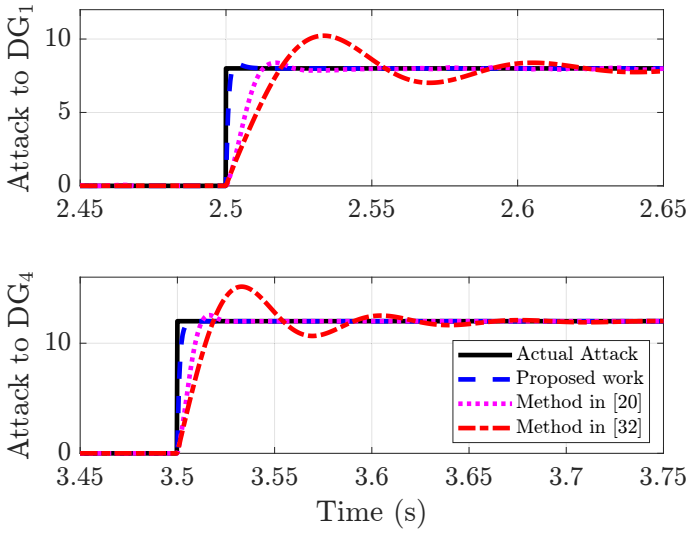


Figure 4.18 . FDIA detection with the proposed method and that developed in [2] and [3].

As shown in Fig 4.18, the proposed approach detects attack signals more rapidly than the schemes described in [2] and [3], reducing the potential impact of these attacks on MGs. The voltage and current profiles of four DGs, illustrated in Fig. 4.19, highlight that attack-induced changes in DG currents are significantly more severe in [2] and [3] compared to our approach. Under these circumstances, the protection system in the other techniques may activate, as the over-current during the

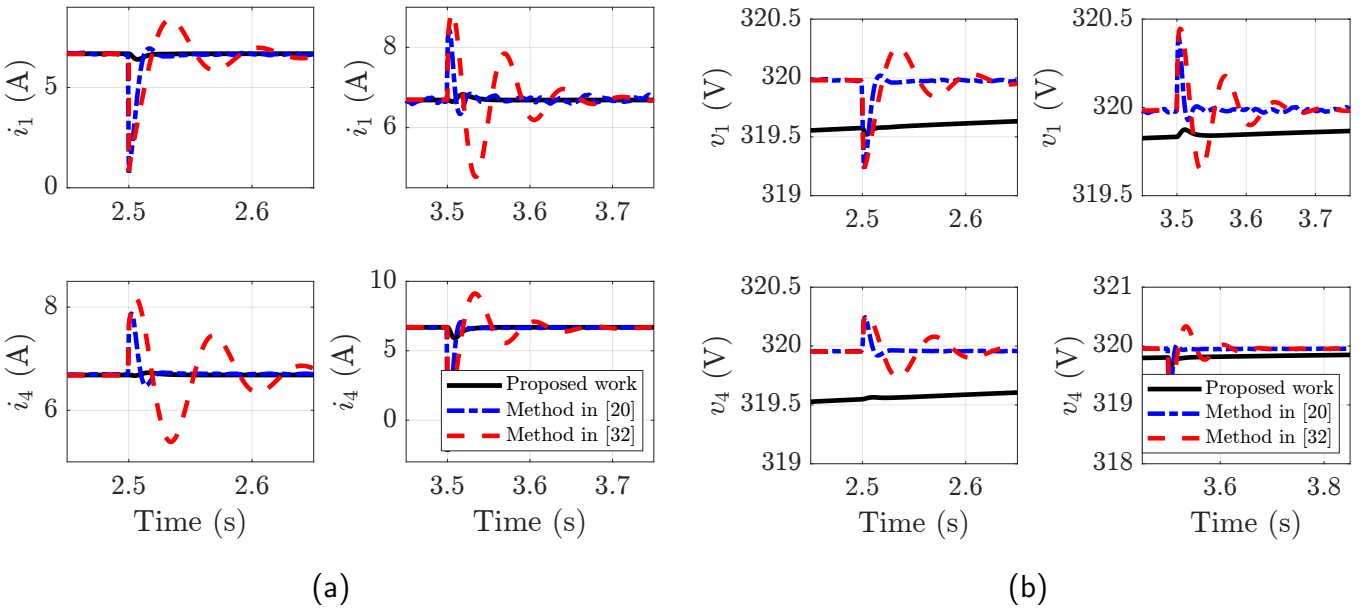


Figure 4.19 . The values of **(a).** currents and **(b).** voltages with the proposed technique and that developed in [2] and [3].

attack can trigger relays.

4.4.7 Comparative study

A comparative study is conducted to show the superiority of the proposed method over other existing methods in the literature. A number of quality features are first defined, and then it is checked whether the proposed method has those specific features compared to other methods or not. Table 4.2 summarizes this comparative study.

According to this comparison table, [49, 88, 89] and [177] are able to detect cyberattacks. However, they do not consider attack mitigation, which is of great importance. Additionally, the performance of our proposed method against load and attack value changes, and unbounded time-varying FDIAs has been evaluated by real-time tests, unlike the methods mentioned above. One of the crucial features of our proposed methodology compared to [2, 49], and [177] is that there is no need for a secure channels. By doing so, the occurrence of new cyberattacks in the communication channels can be avoided. Regarding the reliability features, contrary to [2], where an open loop observer is utilised for power lines current estimation, our proposed methodology used a robust estimator based

Table 4.2 . Comparing the proposed method to other related works

Features \ Methods	[2]	[49]	[88, 89]	[177]	Proposed
Parameter uncertainty	×	✓	✓	×	✓
Scalability	✓	✓	✓	✓	✓
Reliability	×	✓	✓	×	✓
Attack mitigation	✓	×	×	×	✓
Noise measurements	✓	×	✓	✓	✓
No extra channels	×	×	✓	×	✓
Time-varying attacks	✓	×	×	×	✓
Real-time or practical tests	✓	×	×	×	✓

on unknown input observers.

4.5 Summary

This chapter presented the second major contribution of this thesis: addressing FDIAs in dc MGs using a novel PO-based UIO scheme. In this approach, each DG is equipped with a set of PO-based UIOs, enabling state estimation of neighboring DGs without requiring additional communication channels. This design reduces the risk of introducing new cyber-attack vulnerabilities. With this setup, each DG can estimate both the states and FDIAs in the communication links of adjacent units. Identified compromised signals are corrected to ensure data integrity. Moreover, to achieve control objectives in dc MGs, a distributed secondary control system generates the target voltage reference for each DG, while a state-feedback controller with integrator action at the primary control level ensures system stability. This approach is highly scalable, effectively managing cyber-attacks in MGs with any number of DGs without compromising performance. Beyond theoretical validation,

the proposed method's capability to ensure the safe operation of dc MGs under various FDIAs has been demonstrated through real-time OPAL-RT simulation results.

Chapter 5

Cyberattack Reconstruction and Mitigation with a Reduced-Order Unknown Input Observer-Based Approach for AC Microgrids

AC MGs are networks that integrate energy generation sources, storage systems, and loads through power electronic devices. They play a crucial role in enhancing energy reliability, facilitating the integration of renewable energy sources, and optimizing energy costs in modern power systems. AC MGs can operate in both grid-connected and islanded modes, offering flexibility and resilience to the energy infrastructure. A critical challenge in operating ac MGs under FDIAs is ensuring the equitable distribution of active and reactive power among DGs, while maintaining stable and precise voltage and frequency regulation. Building on the unique properties of the scheme introduced in Chapter 4, this chapter extends that method to ac MGs, enabling the safe operation of such systems against a variety of FDIAs.

This chapter improves existing knowledge by addressing critical research gaps and industrial challenges in the cybersecurity of ac MGs. In this regard, a distributed reduced-order PO-based UIO framework has been developed to address FDIAs in ac MGs. This framework reconstructs and mitigates the impact of FDIAs by neutralizing their harmful effects and purifying corrupted communication signals. The principal contributions of this research are summarized as follows:

1. A novel set of reduced-order PO-based UIOs has been proposed to reconstruct cyberattacks in interconnected power and information networks in an ac MG. This approach estimates the states of neighboring DGs without needing additional data exchange between DGs [184, 185, 186, 187].

2. A unified and comprehensive detection/mitigation strategy has been designed for ac MGs with vulnerable information networks, enhancing their resilience and security against FDIAs. The effectiveness of this scheme has been tested under different cyberattack scenarios, including

both constant and dynamic FDIAs, by using real-time detection and corrective measures at the control center.

5.1 Problem formulation: AC MG modeling

This section presents the dynamic model of an ac MG where the j-th DG is depicted in Fig. 5.1. The DG model comprises a dc voltage source connected to a VSC operating as a pulse width modulation inverter. An LC filter is employed to attenuate high-frequency switching harmonics, ensuring the delivery of a clean ac waveform. The output is connected to a three-phase series RLC load, representing the aggregate impedance of the connected devices. Each DG is interconnected with neighboring DGs through power lines characterized by specific resistive and inductive properties, modeling the real-world impedance of electrical distribution lines.

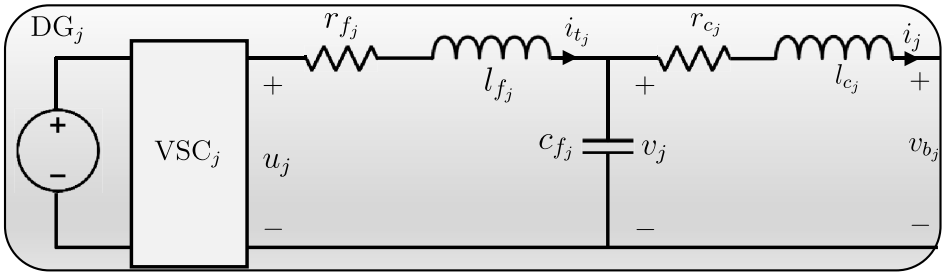


Figure 5.1 . The schematic of j-th inverter-based DG

Assuming continuous mode and employing Kirchhoff's principles, the mathematical representation of the j-th inverter-based DG in *abc*-frame is established as follows:

$$\begin{aligned}
\dot{i}_{t_{abc_j}} &= \frac{1}{l_{f_j}}(u_{abc_j} - v_{abc_j} - r_{f_j} i_{t_{abc_j}}),\\
\dot{v}_{abc_j} &= \frac{1}{c_{f_j}}(i_{t_{abc_j}} - i_{abc_j}),\\
\dot{i}_{abc_j} &= \frac{1}{l_{c_j}}(v_{abc_j} - v_{b_{abc_j}} - r_{c_j} i_{abc_j}),
\end{aligned} \tag{5.1}$$

where $i_{t_{abc_j}}$, v_{abc_j}, and i_{abc_j} represent the generated current, inverter output voltage, and inverter output current, respectively, all of which are measurable. Additionally, l_{f_j}, r_{f_j}, c_{f_j}, and l_{c_j}, r_{c_j} denote the filter inductance, resistance, shunt capacitor, and the inductance and resistance of the output connector, respectively. In (5.1), u_{abc_j} and $v_{b_{abc_j}}$ denote the output voltage of the j-th VSC

and the j-th bus voltage, respectively. Consequently, the output vector for DG_j in abc-frame is expressed as $y_{abc_j} = [i_{t_{abc_j}},\ v_{abc_j},\ i_{abc_j}]^T$.

By applying the Clarke-Park transformation, each equation from (5.1) can be converted to the rotating $dq0$-frame as:

$$\begin{aligned}
\dot{i}_{t_{d_j}} &= \frac{1}{l_{f_j}}(u_{d_j} - v_{d_j} - r_{f_j} i_{t_{d_j}}) + \omega_0 i_{t_{q_j}},\\
\dot{i}_{t_{q_j}} &= \frac{1}{l_{f_j}}(u_{q_j} - v_{q_j} - r_{f_j} i_{t_{q_j}}) - \omega_0 i_{t_{d_j}},\\
\dot{v}_{d_j} &= \frac{1}{c_{f_j}}(i_{t_{d_j}} - i_{d_j}) + \omega_0 v_{q_j},\\
\dot{v}_{q_j} &= \frac{1}{c_{f_j}}(i_{t_{q_j}} - i_{q_j}) - \omega_0 v_{d_j},\\
\dot{i}_{d_j} &= \frac{1}{l_{c_j}}(v_{d_j} - v_{b_{d_j}} - r_{c_j} i_{d_j}) + \omega_0 i_{q_j},\\
\dot{i}_{q_j} &= \frac{1}{l_{c_j}}(v_{q_j} - v_{b_{q_j}} - r_{c_j} i_{q_j}) - \omega_0 i_{d_j}.
\end{aligned} \tag{5.2}$$

Following [188], it is assumed that the angular frequency is controlled in an open loop by equipping each DG with an internal oscillator, which provides Park's transformation angle $\theta(t) = \int_{t_0}^{t} \omega_0 d\tau$, where $\omega_0 = 2\pi f_0$, and f_0 represents the nominal frequency.

5.1.1 Direct power control

In this section, the active and reactive power dynamics of the ac MG are derived. The instantaneous active and reactive power in the $\alpha - \beta$ frame between grid and VSI is represented as follows [188]:

$$\begin{aligned}
p_j &= \frac{3}{2}(v_{b_{\alpha_j}} i_{\alpha_j} + v_{b_{\beta_j}} i_{\beta_j}),\\
q_j &= \frac{3}{2}(v_{b_{\beta_j}} i_{\alpha_j} - v_{b_{\alpha_j}} i_{\beta_j}).
\end{aligned} \tag{5.3}$$

By representing the last relation of (5.1) in $\alpha - \beta$ frame, we have:

$$\begin{aligned}
\dot{i}_{\alpha_j} &= \frac{1}{l_{c_j}}(v_{\alpha_j} - v_{b_{\alpha_j}} - r_{c_j} i_{\alpha_j}),\\
\dot{i}_{\beta_j} &= \frac{1}{l_{c_j}}(v_{\beta_j} - v_{b_{\beta_j}} - r_{c_j} i_{\beta_j}).
\end{aligned} \tag{5.4}$$

Taking the first time derivative of (5.3), the dynamic equations for the instantaneous active and

reactive powers can be expressed as follows:

$$\begin{aligned}\dot{p}_j &= \frac{3}{2}(v_{b_{\alpha_j}}\dot{i}_{\alpha_j} + i_{\alpha_j}\dot{v}_{b_{\alpha_j}} + v_{b_{\beta_j}}\dot{i}_{\beta_j} + i_{\beta_j}\dot{v}_{b_{\beta_j}}),\\ \dot{q}_j &= \frac{3}{2}(v_{b_{\beta_j}}\dot{i}_{\alpha_j} + i_{\alpha_j}\dot{v}_{b_{\beta_j}} - v_{b_{\alpha_j}}\dot{i}_{\beta_j} - i_{\beta_j}\dot{v}_{b_{\alpha_j}}).\end{aligned} \tag{5.5}$$

By considering the point of common coupling (PCC) voltage and angular frequency, we have:

$$\begin{aligned}v_{b_{\alpha_j}} &= v_{pcc_j}\cos(\omega_0 t),\\ v_{b_{\beta_j}} &= v_{pcc_j}\sin(\omega_0 t),\end{aligned} \tag{5.6}$$

where $v_{pcc_j} = \sqrt{v_{b_{\alpha_j}}^2 + v_{b_{\beta_j}}^2}$. By taking the first-time derivative of (5.6), we have:

$$\begin{aligned}\dot{v}_{b_{\alpha_j}} &= -\omega_0 v_{pcc_j}\sin(\omega_0 t) = -v_{b_{\beta_j}}\omega_0,\\ \dot{v}_{b_{\beta_j}} &= \omega_0 v_{pcc_j}\cos(\omega_0 t) = v_{b_{\alpha_j}}\omega_0.\end{aligned} \tag{5.7}$$

By substituting (5.4) and (5.7) into (5.5), and performing mathematical simplifications, the dynamic active and reactive powers can be represented as follows:

$$\begin{aligned}\dot{p}_j &= -\frac{r_{c_j}}{l_{c_j}}p_j - \omega_0 q_j + \frac{3}{2l_{c_j}}u_{p_j},\\ \dot{q}_j &= \omega_0 p_j - \frac{r_{c_j}}{l_{c_j}}q_j + \frac{3}{2l_{c_j}}u_{q_j},\end{aligned} \tag{5.8}$$

where $u_{p_j} = -v_{pcc_j}^2 + v_{\alpha_j}v_{b_{\alpha_j}} + v_{\beta_j}v_{b_{\beta_j}}$ and $u_{q_j} = v_{\alpha_j}v_{b_{\beta_j}} - v_{\beta_j}v_{b_{\alpha_j}}$. Each DG is assumed to be connected to its neighboring units through an undirected communication network without self-loops. Considering (5.2) and (5.8), the dynamic equations of the j-th DG can be expressed in the state-space form as follows:

$$\begin{aligned}\dot{x}_j(t) &= A_j x_j(t) + E_j d_j(t),\\ y_j(t) &= C_j x_j(t),\end{aligned} \tag{5.9}$$

where

$$A_j = \begin{bmatrix} \frac{-r_{f_j}}{l_{f_j}} & \omega_0 & \frac{-1}{l_{f_j}} & 0 & 0 & 0 & 0 & 0 \\ -\omega_0 & \frac{-r_{f_j}}{l_{f_j}} & 0 & \frac{-1}{l_{f_j}} & 0 & 0 & 0 & 0 \\ \frac{1}{c_{f_j}} & 0 & 0 & \omega_0 & \frac{-1}{c_{f_j}} & 0 & 0 & 0 \\ 0 & \frac{1}{c_{f_j}} & -\omega_0 & 0 & 0 & \frac{-1}{c_{f_j}} & 0 & 0 \\ 0 & 0 & \frac{1}{l_{c_j}} & 0 & \frac{-r_{c_j}}{l_{c_j}} & \omega_0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{l_{c_j}} & -\omega_0 & \frac{-r_{c_j}}{l_{c_j}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{-r_{c_j}}{l_{c_j}} & -\omega_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega_0 & \frac{-r_{c_j}}{l_{c_j}} \end{bmatrix}, E_j = \begin{bmatrix} \frac{1}{l_{f_j}} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{l_{f_j}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{l_{c_j}} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{l_{c_j}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{3}{2l_{c_j}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{3}{2l_{c_j}} \end{bmatrix},$$

$$C_j = I_r. \tag{5.10}$$

Here, $x_j(t) = [i_{t_{d_j}}, i_{t_{q_j}}, v_{d_j}, v_{q_j}, i_{d_j}, i_{q_j}, p_j, q_j]^T \in \mathbb{R}^n$ and $y_j(t) \in \mathbb{R}^r$ represent the system state and system output, respectively. It is worth mentioning that $y_j(t) = x_j(t)$, where $n = r$. In this equation, $A_j \in \mathbb{R}^{n\times n}$, $E_j \in \mathbb{R}^{n\times m}$, and $C_j \in \mathbb{R}^{r\times n}$ represent the system, input, and output matrices, respectively. To make the problem more realistic, the output voltages of each VSC (i.e., u_{d_j} and u_{q_j}), the bus voltages of each DG connected to its neighbors (i.e., $v_{b_{d_j}}$ and $v_{b_{q_j}}$), and the active and reactive control inputs (i.e., u_{p_j} and u_{q_j}) are assumed to be unknown to neighboring DGs. Therefore, $d_j(t) = [u_{d_j}, u_{q_j}, v_{b_{d_j}}, v_{b_{q_j}}, u_{p_j}, u_{q_j}]^T$. As a result, all inputs of the DG are assumed to be unknown, eliminating the potential for new cyberattacks arising from the transmission of those signals [79, 160]. This enhances the reliability of the proposed technique. Thus, it is assumed that all exogenous inputs in DG_j [i.e., $E_j d_j(t)$] are unknown to its neighboring DGs, where E_j is a full column rank matrix. As mentioned in *Remark* 3.3, E_j should be a full column rank matrix.

The next section develops the UIO to estimate the states of all neighboring units, even in the presence of unknown inputs. The structure of this methodology is illustrated in Fig. 5.2.

5.2 Projection operator-based UIO system design

This section discusses a set of PO-based UIOs designed to estimate the states of all neighboring units for attack reconstruction purposes within a finite time. In this work, it is assumed that cyberattacks target the sensor channels and are generally formulated as follows:

$$\tilde{y}_j(t) = y_j(t) + D_j a_j(t), \tag{5.11}$$

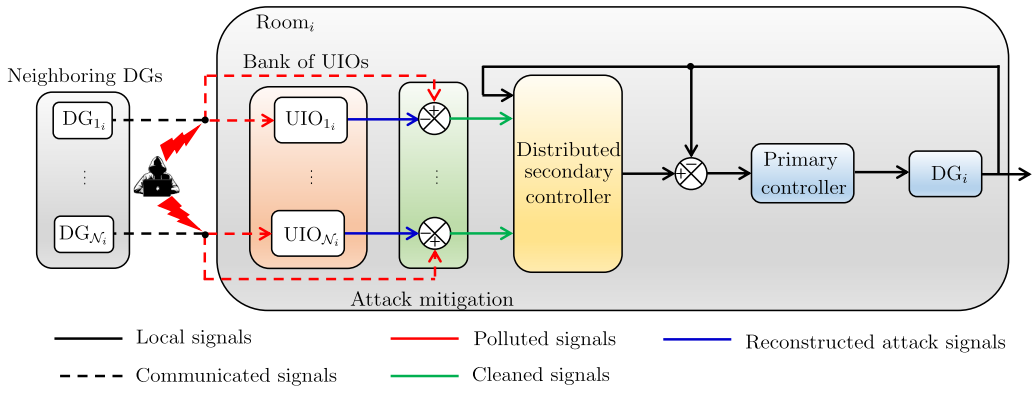


Figure 5.2 . The proposed attack detection/mitigation scheme

where $\tilde{y}_j(t)$ represents the disrupted output signals and $D_j \in \mathbb{R}^{r\times\alpha}$ denotes the attack matrix. Additionally, $a_j(t) \in \mathbb{R}^{\alpha}$ represents the FDIA signals which compromise data integrity by altering the communicated signals through the injection of false data into the communication channels.

In this sequence, the equations for each DG have been augmented by incorporating intruder signals as follows:

$$\begin{aligned} \dot{z}_j(t) &= \bar{A}_j z_j(t) + \bar{E}_j d_j(t), \\ \tilde{y}_j(t) &= \bar{C}_j z_j(t), \end{aligned} \tag{5.12}$$

where $\bar{A}_j \in \mathbb{R}^{(n+\alpha)\times(n+\alpha)}$, $\bar{E}_j \in \mathbb{R}^{(n+\alpha)\times m}$, and $\bar{C}_j \in \mathbb{R}^{r\times(n+\alpha)}$ represent the augmented matrices of appropriate sizes. Additionally, $z_j(t) = [x_j, a_j]^T$ is the augmented state vector, where the FDIA signal a_j is assumed to be a constant scalar. The augmented system matrices are defined as follows:

$$\bar{A}_j = \left[\begin{array}{c|c} A_j & \mathbf{0}_{n\times\alpha} \\ \hline \mathbf{0}_{\alpha\times n} & \mathbf{0}_{\alpha\times\alpha} \end{array}\right], \bar{E}_j = \left[\begin{array}{c} E_j \\ \hline \mathbf{0}_{\alpha\times m} \end{array}\right], \bar{C}_j = \left[\begin{array}{c|c} C_j & D_j \end{array}\right]. \tag{5.13}$$

In the following, the proposed UIO-based scheme is introduced to reconstruct the attack signals.

5.2.1 Proposed reduced-order PO-based attack detection scheme

Considering that $\tilde{y}_j(t)$ is measurable, the states of each DG can be expressed in the following decomposed form:

$$z_j(t) = (I_{(n+\alpha)} - N_j\bar{C}_j)z_j(t) + N_j\bar{C}_j z_j(t) = (I_{(n+\alpha)} - N_j\bar{C}_j)z_j(t) + N_j\tilde{y}_j(t), \tag{5.14}$$

where $N_j \in \mathbb{R}^{(n+\alpha)\times r}$ will be specified later. In the above equation, $z_j(t)$ is decomposed into two parts, that is, the known [i.e., $N_j\tilde{y}_j(t)$] and the unknown [i.e., $\zeta_j(t) = (I_{(n+\alpha)} - N_j\bar{C}_j)z_j(t)$] parts. It can be shown

that with a proper N_j, the dynamics of the unknown parts depend only on the known quantities. For this purpose, we consider $\dot{\zeta}_j(t)$ as:

$$\begin{aligned}\dot{\zeta}_j(t) =&(I_{(n+\alpha)} - N_j\bar{C}_j)\dot{z}_j(t) = (I_{(n+\alpha)} - N_j\bar{C}_j)\left(\bar{A}_j z_j(t) + \bar{E}_j d_j(t)\right)\\ =&(I_{(n+\alpha)} - N_j\bar{C}_j)\bar{A}_j\left(\zeta_j(t) + N_j\tilde{y}_j(t)\right) + (I_{(n+\alpha)} - N_j\bar{C}_j)\bar{E}_j d_j(t).\end{aligned} \tag{5.15}$$

According to (5.15), it is clear that if we choose N_j such that

$$(I_{(n+\alpha)} - N_j\bar{C}_j)\bar{E}_j = 0, \tag{5.16}$$

then the dynamic of ζ_j depends only on the known quantity, i.e., $\tilde{y}_j$. To proceed further, the following condition is required.

Condition 5.1. $\operatorname{rank}\left(\bar{C}_j\bar{E}_j\right) = \operatorname{rank}\bar{E}_j = m$.

To derive the dynamic estimation error, it is assumed that (5.16) holds. A solution to this equation under *Condition* 5.1 is given by:

$$N_j = \bar{E}_j\left(\bar{C}_j\bar{E}_j\right)^{\dagger} = \bar{E}_j(\bar{E}_j^T\bar{C}_j^T\bar{C}_j\bar{E}_j)^{-1}\bar{E}_j^T\bar{C}_j^T, \tag{5.17}$$

where the superscript † is the Moore-Penrose pseudo-inverse operation. It should be noted that (5.17) can be simplified to $N_j = \bar{E}_j(\bar{C}_j\bar{E}_j)^{-1}$ when $\bar{C}_j\bar{E}_j$ is a square matrix, and as a result, it becomes invertible. Thanks to the properties of the Moore-Penrose pseudo-inverse operation (i.e., $\left(\bar{C}_j\bar{E}_j\right)^{\dagger}\left(\bar{C}_j\bar{E}_j\right)\left(\bar{C}_j\bar{E}_j\right)^{\dagger} = \left(\bar{C}_j\bar{E}_j\right)^{\dagger}$ [180]), it can be shown that $N_j\bar{C}_j$ is a projection [i.e., $(N_j\bar{C}_j)^2 = N_j\bar{C}_j$], and as a result, $\check{P}_j = I_{(n+\alpha)} - N_j\bar{C}_j$ is also a projection [182].

Remark 5.1. *Considering* (5.12), $\bar{E}_j d_j(t)$ *encompasses all unknown inputs. By solving* (5.16) *with an appropriate* N_j, (5.15) *can be rewritten as* $\dot{\zeta}_j(t) = (I_{(n+\alpha)} - N_j\bar{C}_j)\bar{A}_j\left(\zeta_j(t) + N_j\tilde{y}_j(t)\right)$, *effectively eliminating the influence of unknown inputs on the state estimation. As a result, there is no need to know the upper bound of these unknown inputs, unlike those methods in [87] and [89].*

To estimate the states of the considered ac MG [i.e., $z_j(t)$], it is required to precisely estimate $\zeta_j(t)$. Thus, we have;

$$\dot{\hat{\zeta}}_j(t) =(I_{(n+\alpha)} - N_j\bar{C}_j)\bar{A}_j\left(\hat{\zeta}_j(t) + N_j\tilde{y}_j(t)\right) + (I_{(n+\alpha)} - N_j\bar{C}_j)\left(L_j\bar{C}_j(z_j(t) - \hat{z}_j(t))\right), \tag{5.18}$$

where $\hat{z}_j(t)$ is assumed as an estimation of $z_j(t)$, and $L_j \in \mathbb{R}^{(n+\alpha)\times r}$ is the observer gain that will be designed later. Let $e_j(t) = z_j(t) - \hat{z}_j(t)$. In *Theorem* 5.1, it will be shown that with the proposed UIO, $e_j(t) \to 0$ as $t \to \infty$. To develop the proposed observer, we need the following lemma.

Lemma 5.1. *Assume that* $\check{P}_j : \mathbb{R}^{(n+\alpha)} \to \mathbb{R}^{(n+\alpha)}$ *is a projection, where* $\operatorname{rank} \check{P}_j = n+\alpha-m$. *Then,* $\check{P}_j$ *has* $(n+\alpha-m)$ *eigenvalues equal to* 1 *and* m *eigenvalues equal to* 0. *In addition, there is a basis,* G_j, *such that:*

$$G_j^{-1}\check{P}_j G_j = P_j = \begin{bmatrix} I_{(n+\alpha-m)} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0}_m \end{bmatrix}, \tag{5.19}$$

where $G_j \in \mathbb{R}^{(n+\alpha)\times(n+\alpha)}$ *is an invertible matrix whose columns are the eigenvectors of matrix* $\check{P}_j$ *[180].*

Remark 5.2. *According to the property of the projection operator expressed in Lemma 5.1, estimating all states of the system is no longer necessary. This feature allows for the simplification for effective decoupling of system states from unknown inputs. Using these projection properties, only the* $(n+\alpha-m)$ *states need to be estimated, while the remaining* m *states can be ignored.*

5.2.2 Reduced-order projection operator-based attack detection

In this section, the proposed reduced-order PO-based UIO is developed. Let's apply the transformation G_j^{-1} to $\hat{\zeta}_j(t)$, as follows:

$$\check{\zeta}_j(t) = G_j^{-1}\hat{\zeta}_j(t). \tag{5.20}$$

Now, by using (5.18), (5.20), and *Lemma* 5.1, we have:

$$\dot{\check{\zeta}}_j(t) = P_j G_j^{-1}\left[\bar{A}_j G_j \check{\zeta}_j(t) + \bar{A}_j N_j \tilde{y}_j(t) + L_j(\tilde{y}_j(t) - \bar{C}_j\hat{\zeta}_j(t) - \bar{C}_j N_j \tilde{y}_j(t))\right]. \tag{5.21}$$

According to (5.20), $\hat{\zeta}_j(t) = G_j\check{\zeta}_j(t)$; thus,

$$\dot{\check{\zeta}}_j(t) = P_j G_j^{-1}\left(\bar{A}_j G_j - L_j\bar{C}_j G_j\right)\check{\zeta}_j(t) + P_j G_j^{-1}\left(\bar{A}_j N_j + L_j - L_j\bar{C}_j N_j\right)\tilde{y}_j(t), \tag{5.22}$$

which can be simplified as follows:

$$\dot{\check{\zeta}}_j(t) = P_j(\check{A}_j - \check{L}_j\check{C}_j)\check{\zeta}_j(t) + P_j G_j^{-1}\left[\left(\bar{A}_j N_j + G_j\check{L}_j\left(I_r - \bar{C}_j N_j\right)\right)\tilde{y}_j(t)\right], \tag{5.23}$$

Now, we can define $\check{\zeta}_j(t) = \begin{bmatrix} \check{\zeta}_{j_1}(t) \\ \check{\zeta}_{j_2}(t) \end{bmatrix}$, where $\check{\zeta}_{j_1} \in \mathbb{R}^{(n+\alpha-m)}$ and $\check{\zeta}_{j_2} \in \mathbb{R}^m$. Thanks to the structure of matrix P_j [see (5.19)] and since this matrix is pre-multiplied to (5.23), we can make sure that $\check{\zeta}_{j_2}(t) = 0$ for $t \geq 0$ provided that $\check{\zeta}_{j_2}(0) = 0$. As a result, by estimating only the first $(n+\alpha-m)$ states with the observer and ignoring the remaining m states, we have:

$$\check{A}_j = G_j^{-1}\bar{A}_j G_j = \begin{bmatrix} \check{A}_{j_{11}} & \check{A}_{j_{12}} \\ \check{A}_{j_{21}} & \check{A}_{j_{22}} \end{bmatrix}, \check{L}_j \ = G_j^{-1}L_j = \begin{bmatrix} \check{L}_{j_1} \\ \check{L}_{j_2} \end{bmatrix}, \ \check{C}_j = \bar{C}_j G_j = \begin{bmatrix} \check{C}_{j_1} & \check{C}_{j_2} \end{bmatrix}. \tag{5.24}$$

Here, $\check{A}_{j_{11}} \in \mathbb{R}^{(n+\alpha-m)\times(n+\alpha-m)}$, $\check{A}_{j_{12}} \in \mathbb{R}^{(n+\alpha-m)\times m}$, $\check{A}_{j_{21}} \in \mathbb{R}^{m\times(n+\alpha-m)}$, $\check{A}_{j_{22}} \in \mathbb{R}^{m\times m}$, $\check{L}_{j_1} \in \mathbb{R}^{(n+\alpha-m)\times r}$, $\check{L}_{j_2} \in \mathbb{R}^{m\times r}$, $\check{C}_{j_1} \in \mathbb{R}^{r\times(n+\alpha-m)}$, and $\check{C}_{j_2} \in \mathbb{R}^{r\times m}$. Concerning $\check{A}_{j_{11}}$ and $\check{C}_{j_1}$ the following assumption is required.

Assumption 5.1. *It is assumed that the pair* $\left(\check{A}_{11}, \check{C}_1\right)$ *is detectable.*

Therefore, the resulting reduced-order observer can be represented as follows:

$$\begin{aligned}\dot{\check{\zeta}}_{j_1}(t) &= \left(\check{A}_{j_{11}} - \check{L}_{j_1}\check{C}_{j_1}\right)\check{\zeta}_{j_1}(t) + \check{S}_j\tilde{y}_j(t),\\ \hat{z}_j(t) &= G_j\begin{bmatrix} I_{(n+\alpha-m)} \\ 0_{m\times(n+\alpha-m)}\end{bmatrix}\check{\zeta}_{j_1} + N_j\tilde{y}_j(t),\end{aligned} \tag{5.25}$$

where

$$\check{S}_j = \left[I_{(n+\alpha-m)}\ 0_m\right] \times G_j^{-1}\bar{A}_jN_j + \check{L}_{j_1}\left(I_r - \bar{C}_jN_j\right),$$

and $\hat{z}_j(t)$ is the state estimation. In (5.25), $\check{L}_{j_1}$ is selected by the pole-placement approach so that the matrix $(\check{A}_{j_{11}} - \check{L}_{j_1}\check{C}_{j_1})$ is Hurwitz.

To simplify the equation representation, the subscript (j) is omitted from the variables.

Theorem 5.1. *Assume that Condition 5.1 and Assumption 5.1 hold true. There exists a gain matrix* L_j *so that the estimation error [i.e.,* $e_j(t)$*] converges to 0 as* $t \to \infty$*.*

Proof: Considering the definition of estimation error [i.e., $e(t) = z(t) - \hat{z}(t)$] and using $\hat{z}(t) = \hat{\zeta}(t) + N\tilde{y}(t)$ along with (5.12) and (5.18), the first time derivative of the estimation error can be represented as follows:

$$\begin{aligned}\dot{e}(t) &= \dot{z}(t) - \dot{\hat{z}}(t) = \left(I_{(n+\alpha)} - N\bar{C}\right)\dot{z}(t) - \dot{\hat{\zeta}}(t)\\ &= \left(I_{(n+\alpha)} - N\bar{C}\right)\left(\bar{A}z(t) + \bar{E}d(t)\right)\\ &- \left(I_{(n+\alpha)} - N\bar{C}\right)\bar{A}\left(\hat{\zeta}(t) + N\tilde{y}(t)\right)\\ &- \left(I_{(n+\alpha)} - N\bar{C}\right)\left(L\bar{C}(z(t) - \hat{z}(t))\right).\end{aligned} \tag{5.26}$$

Thanks to (5.16), (5.26) can be simplified as follows:

$$\begin{aligned}\dot{e}(t) &= \left(I_{(n+\alpha)} - N\bar{C}\right)\bar{A}\left(z(t) - \hat{z}(t)\right) - \left(I_{(n+\alpha)} - N\bar{C}\right)L\bar{C}\left(z(t) - \hat{z}(t)\right)\\ &= \left(I_{(n+\alpha)} - N\bar{C}\right)\left(\bar{A} - L\bar{C}\right)e(t).\end{aligned} \tag{5.27}$$

Now, we need to specify the proper N and L such that $e(t) \to 0$ as $t \to \infty$.

Using the result of *Lemma* 5.1, the following coordinate transformation matrix is introduced:

$$\check{e}(t) = G^{-1}e(t). \tag{5.28}$$

Now, by applying this coordinate transformation matrix to (5.27), we obtain:

$$\dot{\check{e}}(t) = PG^{-1}\left(\bar{A} - L\bar{C}\right)G\check{e}(t). \tag{5.29}$$

By utilising the new matrix definition in (5.24) into (5.29), we obtain:

$$\dot{\check{e}}(t) = P(\check{A} - \check{L}\check{C})\check{e}(t) = \begin{bmatrix} \check{A}_{11} - \check{L}_1\check{C}_1 & \check{A}_{12} - \check{L}_1\check{C}_2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \check{e}_1(t) \\ \check{e}_2(t) \end{bmatrix}, \tag{5.30}$$

where $\check{e}_1(t) \in \mathbb{R}^{(n+\alpha-m)}$ and $\check{e}_2(t) \in \mathbb{R}^m$. As is clear, $\dot{\check{e}}_2(t) = 0$. Thus, it can be concluded that $\check{e}_2(t) = 0$ for $t > 0$, provided that $\check{e}_2(0) = 0$. As a result, (5.30) can be simplified as follows:

$$\dot{\check{e}}_1(t) = \left(\check{A}_{11} - \check{L}_1\check{C}_1\right)\check{e}_1(t). \tag{5.31}$$

Thanks to *Assumption* 5.1, we can find a matrix $\check{L}_1$ such that $\left(\check{A}_{11} - \check{L}_1\check{C}_1\right)$ is Hurwitz. It is clear from (5.31) that $\check{e}_1(t) \to 0$. According to (5.30), it can be concluded that $\check{e}(t) \to 0$. Thus, when $\check{e}_2(t) = 0$, the estimation error of the system is completely dependent on $\check{e}_1(t)$ [See (5.31)]. As a result, it is not required to estimate $\check{e}_2(t)$.

Now, it is required to give a condition on $\hat{\zeta}(0)$ that guarantees that $\check{e}_2(t) = 0$. As previously defined, $\check{P} = I_{(n+\alpha)} - N\bar{C}$; thus, we have:

$$N\bar{C} = I_{(n+\alpha)} - \check{P} = G(I_{(n+\alpha)} - P)G^{-1} \tag{5.32}$$

Thanks to (5.19), we have:

$$I_{(n+\alpha)} - P = \begin{bmatrix} 0_{(n+\alpha-m)} & 0 \\ 0 & I_m \end{bmatrix} \tag{5.33}$$

Using (5.28) and (5.33), $\check{e}_2(t)$ can be obtained as follows:

$$\begin{bmatrix} 0 \\ \check{e}_2(t) \end{bmatrix} = \begin{bmatrix} 0_{(n+\alpha-m)} & 0 \\ 0 & I_m \end{bmatrix} G^{-1}e(t) = G^{-1}N\bar{C}e(t). \tag{5.34}$$

As we know, $e(t) = z(t) - \hat{\zeta}(t) - N\bar{C}z(t)$. Moreover, it was shown that $N\bar{C}$ is a projection operator; thus, we have:

$$\begin{aligned} \begin{bmatrix} 0 \\ \check{e}_2(t) \end{bmatrix} =& G^{-1}N\bar{C}\left(z(t) - \hat{\zeta}(t) - N\bar{C}z(t)\right). \\ =& G^{-1}\left(N\bar{C}z(t) - N\bar{C}\hat{\zeta}(t) - (N\bar{C})^2z(t)\right) \\ =& G^{-1}N\bar{C}\hat{\zeta}(t). \end{aligned} \tag{5.35}$$

Hence, it can be concluded that $\check{e}_2(0) = 0$ if and only if $N\bar{C}\hat{\zeta}(0) = 0$, which is equivalent to

$$\hat{\zeta}(0) = (I - N\bar{C})v. \tag{5.36}$$

for arbitrary $v \in \mathbb{R}^n$. In particular, $\hat{\zeta}(0) = 0$ satisfies the above condition. It is now required to design the observer gain (i.e., $\check{L}_1$). For this purpose, this observer gain is obtained by a Luenberger observer method, which allows locating the poles of the observer in its desired locations. Under *Conditions* 5.1 and *Assumption* 5.1, it can be concluded that the estimation error converges to 0 as $t \to \infty$, which completes the proof. ■

A summary of how the PO-based attack reconstruction scheme can be implemented is provided in the following section. To ensure safe operation of the considered ac MG, it is necessary to equip each DG with a bank of PO-based UIOs. In doing so, all communication signals that may be affected by intruders are cleaned, thereby enabling effective attack mitigation.

5.2.3 Proposed observer implementation

This section discusses how the proposed PO-based UIO can be implemented for an MG. First, it is required to derive the augmented matrices of the under-study ac MG, represented in (5.12). Then, N_j should be calculated with (5.17) to make the dynamic of unknown parts to be dependent on just known quantities. With the proper G_j calculated with (5.19), $\check{A}_j$ and $\check{C}_{j_1}$ should be obtained with (5.24). Afterwards, $\check{L}_{j_1}$ is selected by the pole-placement approach so that the matrix $(\check{A}_{j_{11}} - \check{L}_{j_1}\check{C}_{j_1})$ is Hurwitz. Thanks to the applied transformation and regardless of the number of DGs, the order of each observer is two. To design the gain of the proposed observer, the standard second-order pole placement approach can be used. Then, $\check{L}_j$ and $\check{S}_j$ are calculated. Finally, the proposed PO-based UIO represented by (5.25) will be designed. It should be emphasized that before implementing this scheme, *Conditions* 5.1 and *Assumption* 5.1 are satisfied. A summary of the proposed PO-based state estimation and attack detection is shown in Fig. 5.2 and Algorithm 5.1.

5.3 Control system design

In this section, the design of the control systems, including both primary and secondary controllers, is discussed. The goal is to ensure the overall stability of the ac MG by providing accurate voltage and frequency regulation, as well as proportional active and reactive power sharing among DGs. To achieve this, two cascade PI controllers are implemented in the primary control, along with a distributed secondary controller.

Algorithm 5.1 The proposed PO-based UIO design procedure

Input: Matrices $\bar{A}_j$, $\bar{E}_j$, $\bar{C}_j$, and signal $\tilde{y}_j(t)$.

1: Compute N_j by (5.17).

2: Compute $\check{P}_j$, and G_j with (5.19).

3: Compute $\check{A}_j$, and $\check{C}_j$ with (5.24).

4: Design $\check{L}_{j_1}$ so that $\left(\check{A}_{j_{11}} - \check{L}_{j_1}\check{C}_{j_1}\right)$ is Hurwitz.

5: Compute $\check{S}_j$.

6: Construct the PO-based observer by (5.25).

5.3.1 Distributed secondary control

Following [184], this section discusses a distributed secondary control based on a leader-followers approach to achieve control objectives in ac MGs. In this structure, one DG is designated as the "leader," serving as the autonomous and intelligent reference DG, while all other DGs are considered "followers" of the reference DG. Given the distributed nature of the secondary controller, each DG communicates only with its adjacent units. The control architecture of an autonomous MG is illustrated in Fig. 5.3. The droop control scheme is used to calculate the reference voltage and frequency for each DG to meet the desired objectives [184]. For this purpose, we have:

$$\begin{aligned} \omega_j^\star &= \omega_n - m_{P_j} P_j + \delta\omega_j, \\ v_{d_j}^\star &= v_{d_{ref}} - n_{Q_j} Q_j + \delta v_j, \\ v_{q_j}^\star &= 0. \end{aligned} \tag{5.37}$$

Here, ω_n and $v_{d_{ref}}$ represent the reference frequency and d-component voltage for the entire MG. Additionally, P_j and Q_j denote the measured active and reactive powers, while m_{P_j} and n_{Q_j} are the droop coefficients. Furthermore, $\delta\omega_j$ and δv_j are correction terms used to determine the accurate reference voltage and frequency for each DG. These corrections are calculated within the distributed secondary control system as outlined in [184]:

$$\begin{aligned} \delta\dot{\omega}_j &= K_1 \left(\sum_{i\in\mathcal{N}_j} a_{ji} \left(\omega_i - \omega_j\right) + g_j \left(\omega_n - \omega_j\right) + \sum_{i\in\mathcal{N}_j} a_{ji} \left(m_{P_i} P_i - m_{P_j} P_j\right) \right), \\ \delta\dot{v}_j &= K_2 \left(\sum_{i\in\mathcal{N}_j} a_{ji} \left(n_{Q_i} Q_i - n_{Q_j} Q_j\right) \right), \end{aligned} \tag{5.38}$$

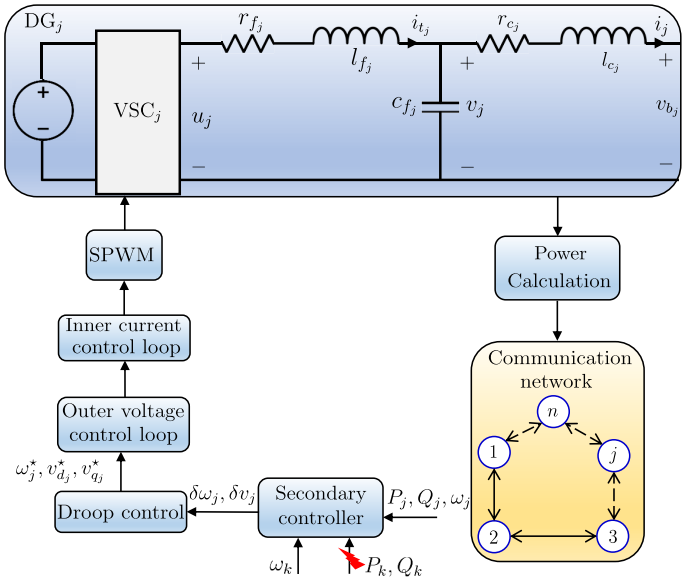


Figure 5.3 . Control structure of the considered ac MG

where $a_{ji} = 1$ when the i-th DG is a neighbor of DG j; otherwise, $a_{ji} = 0$. Additionally, K_1 and K_2 denote the constant gains of the secondary controller. In (5.38), $\mathcal{N}_j$ denotes the set of incident power lines connecting DG$_j$ to its neighboring units. Further analysis of this consensus-based secondary controller can be found in [184].

Remark 5.3. *The secondary control strategy in this work relies on neighboring DGs exchanging active and reactive power, as well as frequency signals, for communication. This dependency makes the system vulnerable to cyberattacks targeting these communication channels. It is assumed that cyberattacks affect the active/reactive power channels, while frequency is transmitted through a secure channel.*

5.3.2 Primary control design

In this section, we develop two cascade PI controllers for the d- and q-components of each DG to ensure the stability of the entire MG. Considering the d-component of the generated current and inverter output voltage [i.e., the first and third relations in (5.2)], the following two transfer functions are derived for the j-th DG. It is important to note that the same procedure is applied to the q-component. Thus, we have the following:

$$\frac{i_{t_{d_j}}(s)}{\frac{1}{l_{f_j}}\left(u_{d_j}(s)-v_{d_j}(s)\right)+\omega_0 i_{t_{q_j}}(s)}=\frac{1}{s+\frac{r_{f_j}}{l_{f_j}}},$$
$$\frac{v_{d_j}(s)}{\frac{1}{c_{f_j}}(i_{t_{d_j}}(s)-i_{d_j}(s))+\omega_0 v_{q_j}(s)}=\frac{1}{s}. \tag{5.39}$$

Considering the reference voltage and frequency magnitudes calculated by the secondary control system for each DG, the primary control is designed to ensure the stability of the entire system. The schematic of this primary control system is illustrated in Fig. 5.4. The gains of these controllers are provided as follows:

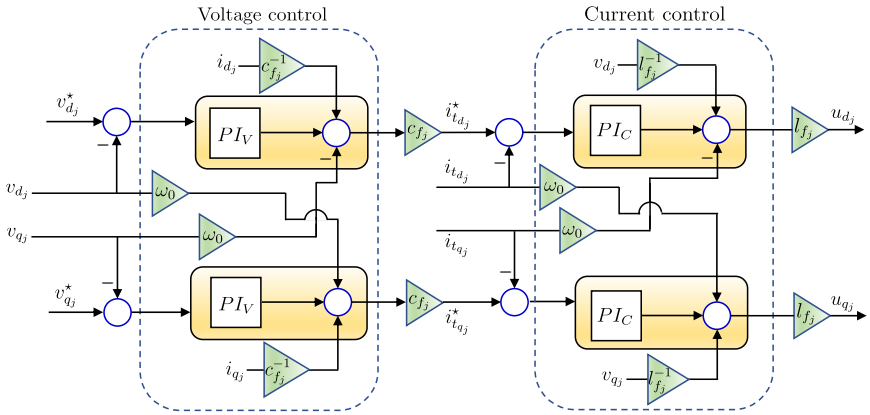


Figure 5.4 . Block diagram of the primary control

$$k_{p_{v_d}}=2\zeta(\omega_n/10) \quad k_{i_{v_d}}=(\omega_n/10)^2,$$
$$k_{p_{i_d}}=2\zeta\omega_n-\frac{r_{f_j}}{l_{f_j}} \quad k_{i_{i_d}}=\omega_n^2, \tag{5.40}$$

where $k_{p_{v_d}}$, $k_{i_{v_d}}$, $k_{p_{i_d}}$, and $k_{i_{i_d}}$ represent the designed proportional and integral gains for the d-component of the inner current and outer voltage control loops. It will be demonstrated that the designed control systems, which include both primary and secondary controls, as well as the proposed attack detection and mitigation schemes, achieve the following objectives [184].

$$\lim_{t\to\infty}||\omega_j(t)-\omega_n||=0 \ \ \forall\, j,$$
$$\lim_{t\to\infty}||m_{P_j}P_j-m_{P_k}P_k||=0 \ \ \forall\, j,k \tag{5.41}$$
$$\lim_{t\to\infty}||n_{Q_j}Q_j-n_{Q_k}Q_k||=0 \ \ \forall\, j,k.$$

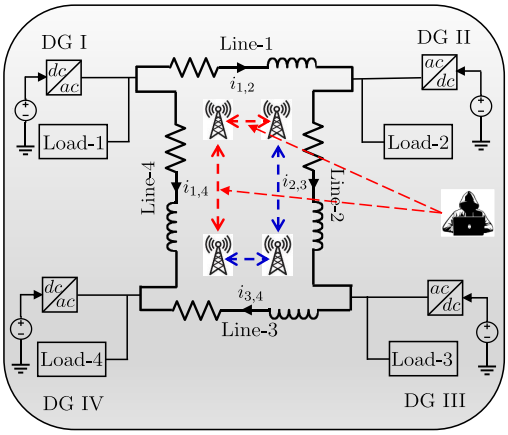


Figure 5.5 . Schematic of the under-study ac MG

The effectiveness of this technique in ensuring the safe operation of ac MGs in the presence of FDIAs is demonstrated in the next section.

5.4 Simulation results

The efficacy of the proposed attack detection and mitigation scheme is evaluated under diverse conditions, such as local load changes and different FDIA behaviors.

5.4.1 Performance evaluation of the proposed scheme

In this section, we evaluate the effectiveness of the proposed scheme against FDIAs using an ac MG consisting of four DGs interconnected by resistive-inductive power lines. The diagram of this MG is shown in Fig. 5.5. It is assumed that the capacity of the odd-numbered DGs (i.e., DG_1 and DG_3) is twice that of the even-numbered DGs (i.e., DG_2 and DG_4). Table 5.1 lists all the parameter values for the considered ac MG.

Figure 5.6 illustrates the active and reactive power outputs, frequency, and d-component of the voltage of all DG units under constant FDIAs. This figure clearly shows that, in the absence of mitigation strategies, these cyberattacks prevent the MG from achieving its intended operational objectives. In this simulation, constant FDIAs are applied to both active and reactive power of DG_2 and DG_4. In this regard, a constant FDIA ($a_{p_2} = 7\ kW$) at $t = 8$s, and a constant FDIA ($a_{p_4} = 20\ kW$) at $t = 7$s are applied to the active power channels of DG_2 and DG_4, respectively. Moreover, a constant FDIA ($a_{q_2} = 6\ kVAr$) at $t = 5$s, and a constant FDIA ($a_{q_4} = 15\ kVAr$) at $t = 4$s are applied to the reactive power channels of DG_2 and DG_4, respectively. As is clear, after the attack signals are applied to the active power at 7 and 8 seconds, the active power

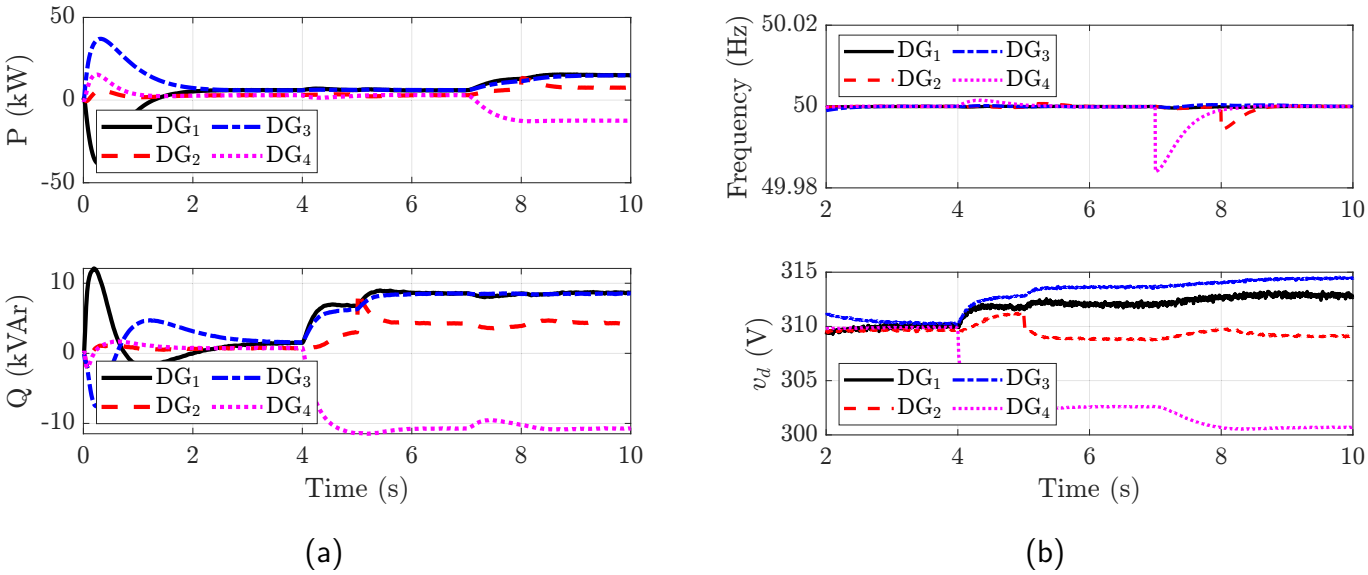


Figure 5.6 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under constant FDIAs without our proposed scheme.

outputs of the DGs diverge and fail to maintain equal power sharing. Due to the nature of droop control, the frequency of the DGs is also affected during these time intervals. Similarly, when attack signals are applied to the reactive power at 4 and 5 seconds, the reactive power sharing among DGs becomes unequal. Again, as a result of droop control, the d-component of the voltage is influenced during these instances. The results highlight that voltage/frequency regulation and accurate active/reactive power sharing are compromised, underscoring the critical need for effective attack detection and mitigation protocols.

After observing the impact of FDIAs on the ac MG in the absence of a detection mechanism, the proposed strategy is applied to reconstruct the attack signals and eliminate the effects of attacks. As shown in Fig. 5.7, which presents the active/reactive powers, as well as the frequency and d-component of the voltage for all DGs, the proposed UIO-based scheme effectively detects and mitigates FDIAs. This figure depicts that the proposed method can effectively address FDIAs. It is evident that both active and reactive powers are properly shared among the DGs. In addition, the frequency is regulated at 50 Hz, and the voltage is maintained at 310 V, confirming the effectiveness of the proposed scheme in detecting and mitigating constant attack signals. Additionally, Fig. 5.8 illustrates the actual profile of cyberattacks alongside their estimated counterparts, confirming the effectiveness of our proposed local observer for attack reconstruction. As shown, the attack is identified promptly after its occurrence, preventing it from affecting the system's

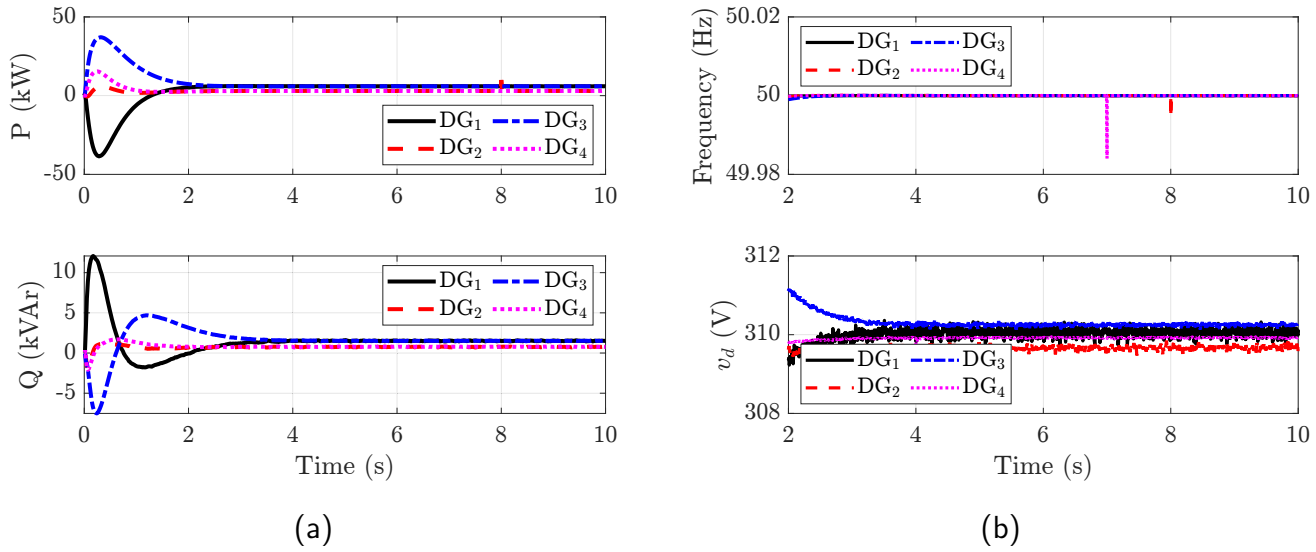


Figure 5.7 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under constant FDIAs with our proposed scheme.

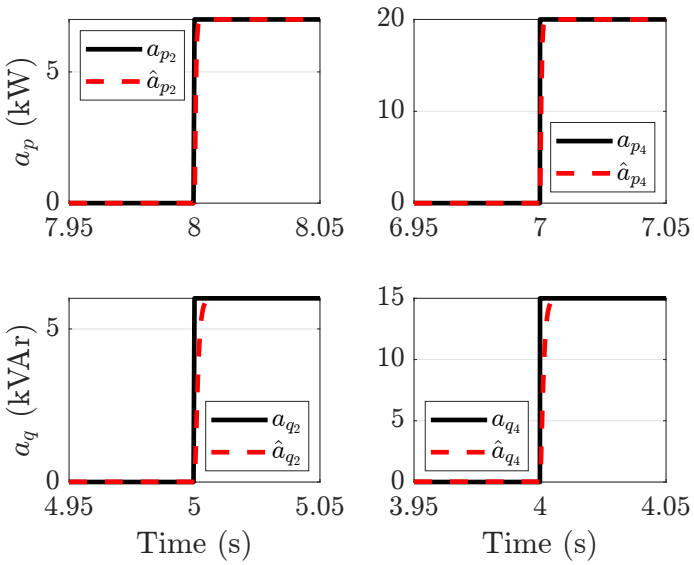


Figure 5.8 . FDIA detection with the proposed UIO strategy.

response.

Table 5.1 . Parameters for the four-DG ac MG simulations

Symbol \ Unit	DG_1	DG_2	DG_3	DG_4
r_{f_j} (Ω)	0.2	0.15	0.25	0.4
l_{f_j} (mH)	8	10	12	18
c_{f_j} (mF)	0.15	0.2	0.25	0.38
r_{c_j} ($m\Omega$)	5	3	4	2.5
l_{c_j} (mH)	0.35	0.5	0.65	0.8
m_P	$2.5e^{-6}$	$5e^{-6}$	$2.5e^{-6}$	$5e^{-6}$
n_Q	$0.1e^{-3}$	$0.2e^{-3}$	$0.1e^{-3}$	$0.2e^{-3}$
Active power (kW)	5	4	5.5	3.5
Reactive power (kVAr)	1.2	1	1.5	0.9

5.4.2 Performance evaluation under time-varying attacks

Cyber-attack signals can be unbounded since they are deliberately designed to cause maximum damage. As a result, any proposed scheme should be assessed for its effectiveness in handling time-varying, unbounded cyber-attacks. In this section, to verify that the proposed scheme can deal with unbounded attacks, we tested our proposed method specifically against time-varying unbounded cyber-attacks. In this scenario, an unbounded FDIA ($a_{p_4} = 0.5t\ kW$) at $t = 7$s, and a time-varying sinusoidal FDIA ($a_{p_2} = 15\sin(5t)\ kW$) at $t = 8$s are applied to the active power channels of DG_4 and DG_2, respectively. Moreover, a time-varying unbounded FDIA ($a_{q_4} = t\ kVAr$ for $4 \leq t < 8$ and $a_{q_4} = (8-t)\ kVAr$ for $t \geq 8$), and a time-varying sinusoidal FDIA ($a_{q_2} = 5\sin(10t)\ kVAr$) at $t = 5$s are applied to the reactive power channels of DG_4 and DG_2, respectively. Figure 5.9 illustrates the active and reactive power outputs, frequency, and d-component of the voltage of all DG units under these FDIAs. This figure clearly shows that, in the absence of mitigation strategies, these cyberattacks prevent the MG from achieving its intended operational objectives, represented by (5.41). As shown, the active power is compromised by cyberattacks at 7 and 8 seconds. According to the droop control mechanism, this disturbance also impacts the frequency of each DG. As a result, power sharing among the DGs is significantly degraded. Similarly, when the reactive power of each DG is targeted by cyberattacks, the d-component of the voltage is adversely affected. These achieved results highlight that

voltage/frequency regulation and accurate active/reactive power sharing are compromised, underscoring the critical need for effective attack detection and mitigation protocols.

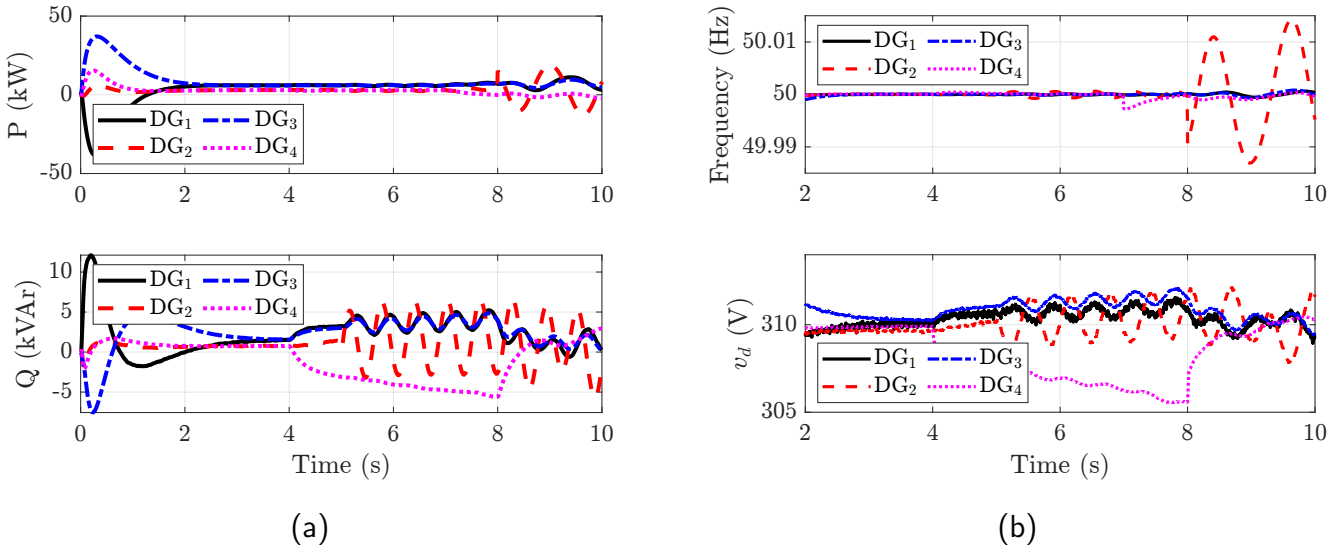


Figure 5.9 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under time-varying FDIAs without our proposed scheme.

To countermeasure the FDIA signals on the ac MG, the proposed strategy is employed to reconstruct the attack signals and mitigate their destructive impacts. Figure 5.10 demonstrates the active/reactive powers, frequency, and d-component of the voltage across all DGs, showcasing the ability of the UIO-based scheme to accurately detect and counteract these time-varying FDIAs. When the attack detection and mitigation mechanism is active, both active and reactive powers are shared equally among the DGs. Also, the frequency and the d-component of voltage of each DG is regulated accurately. Furthermore, Fig. 5.11 compares the actual time-varying cyberattack profiles with their estimated counterparts, confirming the efficiency of the proposed local observer in reconstructing attack signals.

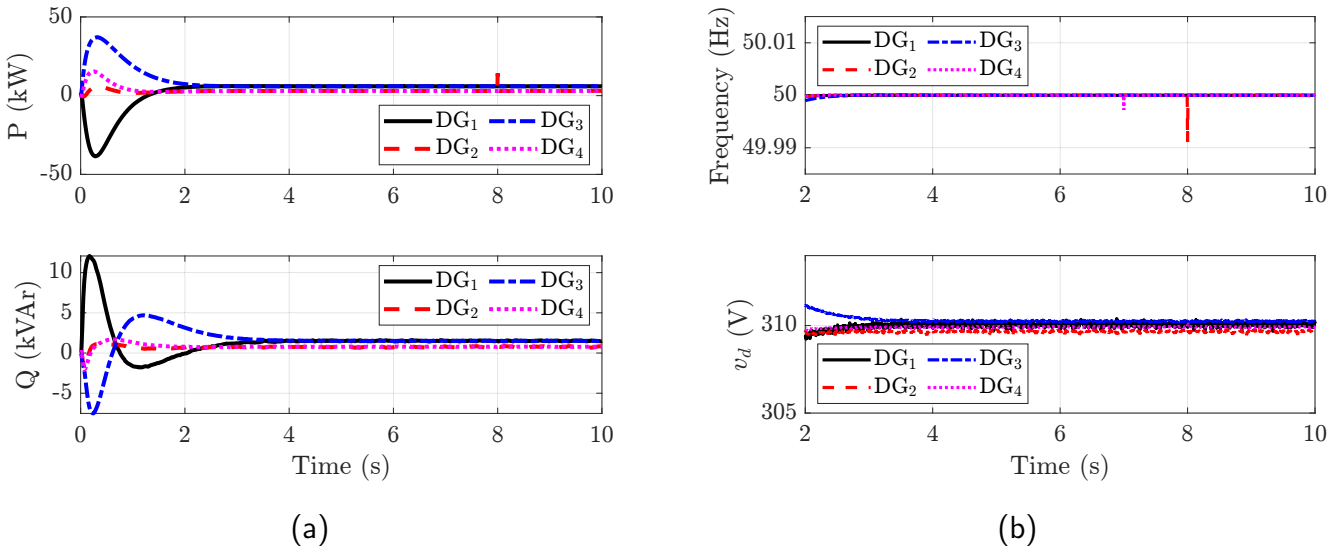


Figure 5.10 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under time-varying FDIAs with our proposed scheme.

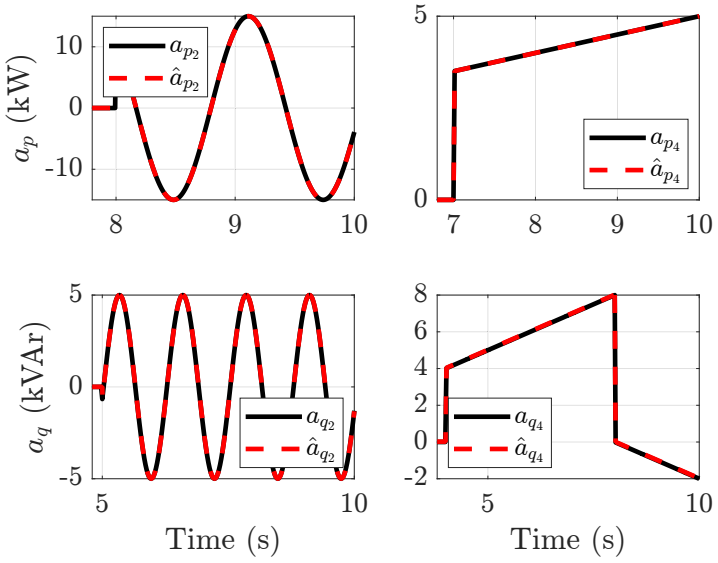


Figure 5.11 . Time-varying FDIA detection with the proposed UIO strategy.

5.4.3 Performance evaluation under varying loads and attack conditions

In this section, a new scenario is introduced to evaluate the effectiveness of the proposed scheme in dealing with both planned and unplanned events, such as variations in local loads and attack magnitudes.

During network operation, local loads at each DG unit may change unexpectedly, potentially affecting system performance. In this scenario, the attack signal on the active power of DG_2 and DG_4 transitions as follows: for DG_2, the signal changes from a sinusoidal waveform ($a_{p_2} = 15\sin(5t)\ kW$) to a ramp waveform ($a_{p_2} = 2t\ kW$) at $t = 3$ s; for DG_4, it changes from a constant value ($a_{p_4} = 8\ kW$) to a sinusoidal waveform ($a_{p_4} = 10\sin(8t)\ kW$) at $t = 5$ s. Similarly, the attack signal on the reactive power of DG_2 and DG_4 changes as follows: for DG_2, the signal transitions from a ramp waveform ($a_{q_2} = 2t\ kVAr$) to a constant value ($a_{q_2} = 25\ kVAr$) at $t = 4$ s; for DG4, it transitions from a sinusoidal waveform ($a_{q_4} = 10\sin(8t)\ kVAr$) to a constant value ($a_{q_4} = 12\ kVAr$) at $t = 6$ s. Additionally, it is assumed that new loads are added to DG_2 and DG_4 at $t = 8$ s and $t = 10$ s, respectively. The new loads are specified as $L_2 = 2\ kW + 0.5\ kVAr$ for DG_2 and $L_4 = 3.5\ kW + 1.2\ kVAr$ for DG_4. As depicted in Fig. 4.12(a) and (b), which present the active/reactive powers and voltage/frequency across all DGs, the MG under study fails to maintain its performance under these conditions. This highlights the critical importance of implementing the proposed detection and mitigation scheme.

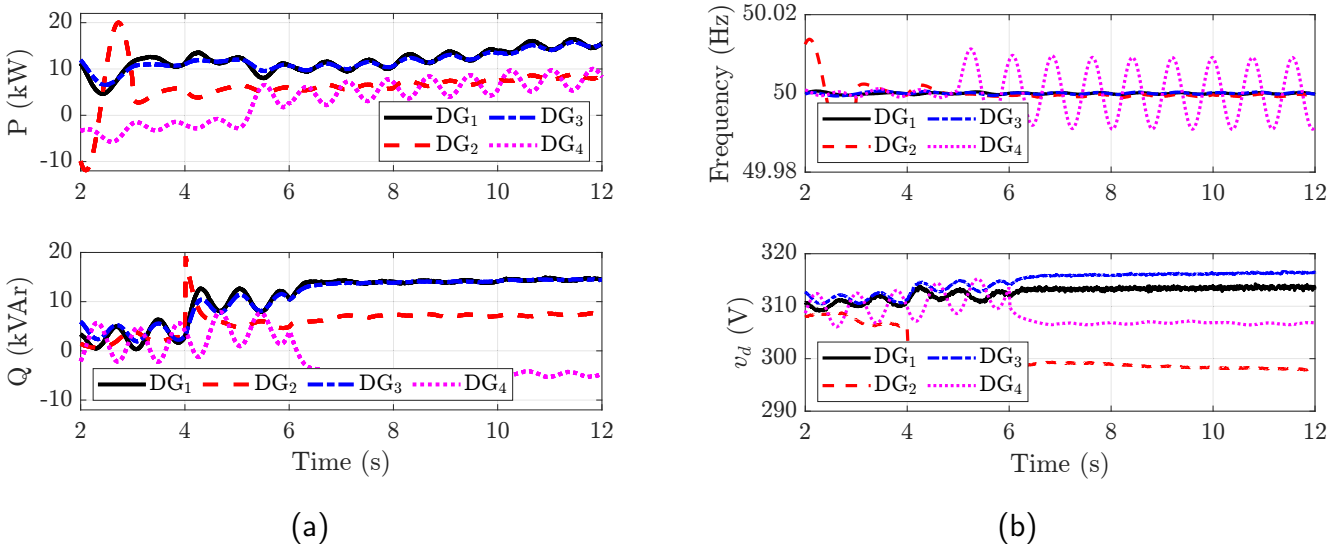


Figure 5.12 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under time-varying FDIAs and load changes without our proposed scheme.

The proposed strategy is applied to tackle the effects of FDIAs on this ac MG. By reconstructing the attack signals, it effectively eliminates their destructive impact. Figure 5.13 illustrates the active/reactive power, frequency, and d-axis voltage across all DGs, demonstrating the capability of the UIO-based approach to identify and neutralize FDIAs with precision. Additionally, Fig. 5.14 contrasts the original cyberattack

signals with their estimated versions, validating the performance of the proposed local observer in reconstructing these attack signals.

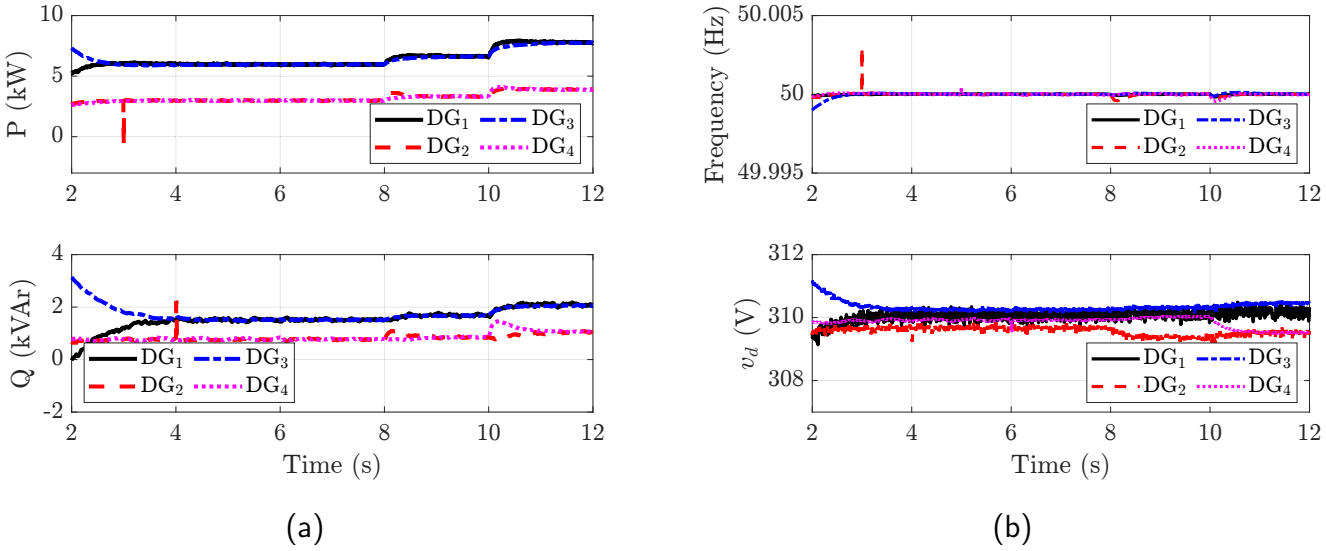


Figure 5.13 . **(a).** The value of active/reactive power, and **(b).** voltage/frequency for all DGs under time-varying FDIAs and load changes with our proposed scheme.

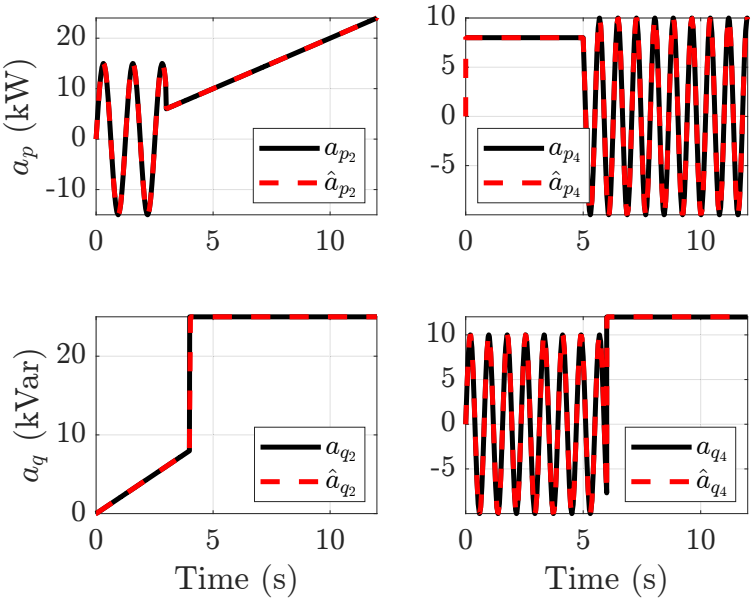


Figure 5.14 . Time-varying FDIA detection with the proposed UIO strategy.

5.4.4 Comparative study

This study includes a comparison to demonstrate the advantages of the proposed method over other existing approaches. Several quality attributes are initially established, and the presence of these attributes in the proposed method is then evaluated relative to other methods. Table 5.2 presents a summary of this comparison.

Table 5.2 . Comparing the proposed method to others

Features \ Methods	[101]	[78]	[189]	[79]	This work
Parameter uncertainty	✓	×	×	×	✓
Scalability	✓	✓	✓	✓	✓
Reliability	✓	×	✓	×	✓
Attack mitigation	✓	✓	✓	✓	✓
Noise measurements	✓	✓	✓	×	✓
Time-varying attacks	×	✓	✓	✓	✓
Real-time or practical tests	✓	✓	×	✓	✓

According to Table 5.2, the proposed method demonstrates a comprehensive advantage over the compared methods by addressing a wide range of critical features. Unlike [78, 189, 79], it effectively handles parameter uncertainty, making it robust against system variations. It ensures scalability, similar to [101, 78, 189, 79], and provides reliable performance, unlike [78, 79]. The method incorporates advanced attack mitigation strategies and successfully addresses time-varying attacks, surpassing [101] in this regard. Additionally, it accounts for noise measurements, unlike [79]. Most importantly, the proposed method has been validated through real-time or practical tests, setting it apart as a reliable and ready-to-deploy solution. This combination of features makes it a versatile and robust approach for modern applications.

5.5 Summary

In this chapter, we extended the observer-driven strategy previously developed in Chapter 4, with modifications to address cybersecurity challenges in ac MGs. For this purpose, each inverter-based DG unit is equipped with a set of UIOs to monitor the states of neighboring units. By incorporating attack signals into the DG equations, the observer system is capable of reconstructing various FDIA signals. Detected attacks are mitigated by subtracting them from the compromised signals, ensuring data integrity. To further enhance system resilience, we established a decentralized secondary control framework to calculate reference voltage and frequency levels. This framework ensures precise frequency regulation and equitable sharing of active and reactive power among DGs. Simulation results demonstrate the effectiveness of this modified approach in safeguarding ac MGs against a range of FDIAs, validating its ability to ensure secure and stable operation.

Chapter 6

Conclusion and Future Works

With the growing demand for energy, MGs have emerged as a reliable and promising solution. However, despite their numerous advantages, MGs remain highly susceptible to adverse factors such as external disturbances, faults, and cyber-attacks, which can threaten their stable operation. Consequently, developing strategies to ensure the safe performance of these systems is of critical importance in both academic and practical contexts. The primary objective of this thesis is to propose innovative solutions to secure the stable performance of compromised dc/ac MGs. This chapter provides a summary of the contributions of this thesis and outlines future directions to improve this research.

6.1 Conclusion

This thesis begins with a comprehensive literature review on cybersecurity in MGs in Chapter 2. Cybersecurity is categorized into two main approaches: attack detection and mitigation schemes, and cyber-resilient control system design. By analyzing these two streams, existing research gaps are identified. Furthermore, this chapter proposes the research questions and defines the objectives of the thesis.

In Chapter 3, a novel model-based scheme is proposed to address various FDIAs in dc MGs. The real-time simulation results, along with a rigorous mathematical proof, demonstrate the effectiveness of this approach. The method consists of two primary layers: (a) attack detection using a SM-based UIO technique, and (b) attack mitigation by filtering out compromised signals. At the reconstruction stage, a robust SM-UIO-based framework is developed to identify attack signals transmitted from neighboring units via communication channels. The primary objectives of dc MGs, that is, accurate voltage regulation and proportional current sharing, are achieved with a distributed secondary control system and two cascade PI controllers in the primary control level. This scheme requires two key components: transmitting one signal through a secure channel and knowing the upper bound of unknown inputs. These limitations are addressed in the next chapter through the development of an enhanced UIO-based attack reconstruction scheme.

In Chapter 4, an innovative PO-based UIO method is introduced to reconstruct and mitigate FDIAs in dc MGs. Each DG is equipped with a set of PO-based UIOs, allowing for state estimation of neighboring

DGs without requiring additional communication channels, thereby reducing the risk of new cyber-attacks. With this setup, each DG can estimate the states and FDIAs in communication links of adjacent units. Any identified compromised signals are then corrected to ensure data integrity. Compared to the SM-based UIO developed in Chapter 3, this method does not require knowing the upper bound of unknown inputs, which enhances its applicability against various FDIAs. To achieve control objectives in dc MGs, a distributed secondary control system generates the target voltage reference for each DG, while a state-feedback control with integrator action in the primary control layer ensures stability. Real-time results using OPAL-RT, along with mathematical proof, confirm the effectiveness of this approach in maintaining secure operations against different kinds of FDIAs.

Chapter 5 developed the observer-driven strategy, introduced in Chapter 4, to address the cybersecurity issue in ac MGs. In this regard, each DG is equipped with a set of PO-based UIOs to monitor the conditions of neighboring units. By incorporating attack signals into the DG equations, our observer system can detect and reconstruct various FDIA signals. Detected attack signals are then neutralized by subtracting them from the corrupted signals. This approach is scalable, effectively managing cyber-attacks in MGs with any number of DGs without diminishing system performance. Additionally, we established a decentralized secondary control framework to determine reference voltage and frequency levels, ensuring precise frequency regulation and equitable distribution of active and reactive power among DGs. Similarly, the simulation results, as well as mathematical proof, validate the effectiveness of this approach in protecting ac MGs against different kinds of FDIAs.

6.2 Recommendations and future works

Based on the contributions of this work, the following directions for future works are suggested:

1. DoS attack is another kind of attacks that affect the normal operation of MGs through blocking the transmission of communicated signals. Developing the proposed UIO-based schemes to immune dc/ac MGs against this class of attacks would be highly beneficial.

2. As mentioned in Chapter 3, it is required to know the upper bound of unknown inputs. As a future direction to improve this method, the SM-based UIO approach can be modified with an adaptive law to calculate the observer's gain, which enhances the applicability of this scheme against various scenarios.

3. As outlined in Chapter 3, the stability of the proposed scheme is mathematically demonstrated only for constant cyber-attacks. However, through various real-time simulation results, the scheme's per-

formance is evaluated against a range of cyber-attacks, including time-varying, unbounded, and sinusoidal FDIAs. Future work could focus on extending the stability analysis to encompass time-varying cyber-attacks, which would significantly enhance the effectiveness of the proposed scheme.

4. As explained in Section 3.2.1, cybersecurity of dc/ac MGs is achieved through developing an unknown input-based observer. As a future direction, developing more advanced and robust control systems, such as sliding mode control and H_∞ control, is suggested to guarantee the robustness of the system against various disturbances and uncertainties.

5. As mentioned in Chapter 4, the proposed detection scheme is limited by the observer bandwidth. Thus, to ensure the observer bandwidth is effectively designed, incorporating more advanced and resilient control strategies, such as adaptive observer gain adjustments, may improve the system's tolerance to fast attack signals.

6. In Section 4.4.4, the effectiveness of the proposed scheme is illustrated in real communication. Validating the proposed approach in converter-based MGs by considering sensor constraints is recommended.

7. In this research, cybersecurity of a single dc and ac MG is taken into account. As a result, cyber-attack is just applied to secondary control system. As a future work, cybersecurity of network MGs is recommended. In this case, intruders can affect both secondary and tertiary control levels, which makes the problem more challenging.

8. Artificial intelligent (AI)-based methods have gained significant attention for enhancing cybersecurity in microgrids, particularly in attack detection and mitigation. Machine learning and deep learning techniques have been employed to identify anomalous patterns in measurement data, enabling real-time intrusion detection. AI-driven approaches, such as reinforcement learning, have also been explored for adaptive defence mechanisms, allowing the system to dynamically adjust its response to evolving cyber threats. In the context of observer-based detection schemes, AI can complement traditional methods by improving feature extraction, reducing false alarms, and enhancing detection accuracy. For instance, integrating AI with the proposed SMO and PO-based UIO framework could refine state estimation by learning complex relationships between system states and cyber anomalies. Additionally, AI techniques can aid in predicting potential attack strategies, thereby enabling proactive mitigation strategies. Future work could explore hybrid models that combine AI-driven anomaly detection with observer-based techniques to further improve the resilience of MGs against cyberattacks.

Bibliography

[1] A. M. Mohan, N. Meskin, and H. Mehrjerdi, "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems," *Energies*, vol. 13, no. 15, p. 3860, 2020.

[2] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads," *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9565–9577, 2021.

[3] L. B. Freidovich and H. K. Khalil, "Performance recovery of feedback-linearization-based designs," *IEEE Transactions on Automatic Control*, vol. 53, no. 10, pp. 2324–2334, 2008.

[4] "Australia's energy strategies and frameworks." *[Online]. Available: https://www.energy.gov.au/government-priorities/australias-energy-strategies-and-frameworks.*

[5] "National energy performance strategy," *[Online]. Available: https://www.energy.gov.au/government-priorities/australias-energy-strategies-and-frameworks/national-energy-performance-strategy.*

[6] "Australian energy statistics." *[Online]. Available: https://www.energy.gov.au/publications/australian-energy-statistics-table-o-electricity-generation-fuel-type-2021-22-and-2022.*

[7] "Net zero." *[Online]. Available: https://www.dcceew.gov.au/climate-change/emissions-reduction/net-zero.*

[8] H. B. Eluri and M. G. Naik, "Challenges of RES with integration of power grids, control strategies, optimization techniques of microgrids: A review," *International Journal of Renewable Energy Research (IJRER)*, vol. 11, no. 1, pp. 1–19, 2021.

[9] A. M. Annaswamy and M. Amin, "IEEE vision for smart grid controls: 2030 and beyond," *IEEE Press, 2013.*

[10] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.

[11] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.

[12] H. Shafei, L. Li, and R. P. Aguilera, "A comprehensive review on cyber-attack detection and control of microgrid systems," *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*, pp. 1–45, 2023.

[13] C. Wang, T. Zhang, F. Luo, F. Li, and Y. Liu, "Impacts of cyber system on microgrid operational reliability," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 105–115, 2017.

[14] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[15] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, vol. 5, no. 1, 2009.

[16] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[17] X. Cao, C. Wei, J. Li, L. Yang, D. Zhang, and G. Tang, "The geological disasters defense expert system of the massive pipeline network scada system based on FNN," in *Asia-Pacific Web Conference*. Springer, 2012, pp. 19–26.

[18] K. E. Hemsley and E. Fisher, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2018.

[19] J. A. Lewis, "Significant cyber incidents since 2006," *Center for Strategic and International Studies*, 2013.

[20] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.

[21] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[22] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[23] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3780–3790, 2018.

[24] A. Villalonga, G. Beruvides, F. Castano, and R. E. Haber, "Cloud-based industrial cyber-physical system for data-driven reasoning: A review and use case on an Industry 4.0 pilot line," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5975–5984, 2020.

[25] S. Tan, Y. Wu, P. Xie, J. M. Guerrero, J. C. Vasquez, and A. Abusorrah, "New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience," *IEEE Electrification Magazine*, vol. 8, no. 4, pp. 98–106, 2020.

[26] S. Madichetty and S. Mishra, "Cyber attack detection and correction mechanisms in a distributed dc microgrid," *IEEE Transactions on Power Electronics*, vol. 37, no. 2, pp. 1476–1485, 2021.

[27] R. Shirey, "Internet security glossary," Tech. Rep., 2000.

[28] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, 2015.

[29] P. B. Hansen, *Operating system principles*. Prentice-Hall, Inc., 1973.

[30] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, pp. 380–388.

[31] D. Liu and D. Ye, "Cluster synchronization of complex networks under denial-of-service attacks with distributed adaptive strategies," *IEEE Transactions on Control of Network Systems*, 2021.

[32] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for dc microgrid system under DoS and impulsive FDI attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3742–3754, 2021.

[33] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[34] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[35] D. Li, P. Ramanan, N. Gebraeel, and K. Paynabar, "Deep learning based covert attack identification for industrial control systems," in *2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2020, pp. 438–445.

[36] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.

[37] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids—a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.

[38] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, 2015.

[39] C.-H. Lo and N. Ansari, "Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33–44, 2013.

[40] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, 2019.

[41] H. Tu, Y. Xia, K. T. Chi, and X. Chen, "A hybrid cyber attack model for cyber-physical power systems," *IEEE Access*, vol. 8, pp. 114 876–114 883, 2020.

[42] A. Basati, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, and S. Golestan, "A data-driven framework for FDI attack detection and mitigation in dc microgrids," *Energies*, vol. 15, no. 22, p. 8539, 2022.

[43] I. Zografopoulos and C. Konstantinou, "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE Transactions on Industrial Informatics*, 2021.

[44] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with PVs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[45] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple dc microgrid clusters," *Applied Energy*, vol. 310, p. 118425, 2022.

[46] Y. Liu and L. Cheng, "Relentless false data injection attacks against Kalman filter based detection in smart grid," *IEEE Transactions on Control of Network Systems*, 2022.

[47] M. S. Ghafoori and J. Soltani, "Designing a robust cyber-attack detection and identification algorithm for dc microgrids based on Kalman filter with unknown input observer," *IET Generation, Transmission & Distribution*, 2022.

[48] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "On addressing the security and stability issues due to false data injection attacks in dc microgrids—an adaptive observer approach," *IEEE Transactions on Power Electronics*, vol. 37, no. 3, pp. 2801–2814, 2021.

[49] H. H. Alhelou and P. Cuffe, "A dynamic-state-estimator-based tolerance control method against cyber-attack and erroneous measured data for power systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4990–4999, 2021.

[50] S. Soltani, M. Kordestani, P. K. Aghaee, and M. Saif, "Improved estimation for well-logging problems based on fusion of four types of Kalman filters," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 56, no. 2, pp. 647–654, 2017.

[51] A. Paul, I. Kamwa, and G. Joos, "Centralized dynamic state estimation using a federation of extended Kalman filters with intermittent PMU data from generator terminals," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6109–6119, 2018.

[52] G. Anagnostou and B. C. Pal, "Derivative-free Kalman filtering based approaches to dynamic state estimation for power systems with unknown inputs," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 116–130, 2017.

[53] Y. Li, Z. Li, and L. Chen, "Dynamic state estimation of generators under cyber attacks," *IEEE Access*, vol. 7, pp. 125 253–125 267, 2019.

[54] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[55] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4281–4292, 2019.

[56] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951–7962, 2019.

[57] J. Qi, A. F. Taha, and J. Wang, "Comparing Kalman filters and observers for power system dynamic state estimation with model uncertainty and malicious cyber attacks," *IEEE Access*, vol. 6, pp. 77 155–77 168, 2018.

[58] M. Adeli, M. Hajatipour, M. J. Yazdanpanah, M. Shafieirad, and H. Hashemi-Dezaki, "Distributed trust-based unscented Kalman filter for non-linear state estimation under cyber-attacks: The application of manoeuvring target tracking over wireless sensor networks," *IET Control Theory & Applications*, vol. 15, no. 15, pp. 1987–1998, 2021.

[59] J. Lu, W. Wang, L. Li, and Y. Guo, "Unscented Kalman filtering for nonlinear systems with sensor saturation and randomly occurring false data injection attacks," *Asian Journal of Control*, vol. 23, no. 2, pp. 871–881, 2021.

[60] X. Liu, Y. Mo, and E. Garone, "Local decomposition of Kalman filters and its application for secure state estimation," *IEEE Transactions on Automatic Control*, vol. 66, no. 10, pp. 5037–5044, 2020.

[61] S. Saha, T. Roy, M. Mahmud, M. Haque, and S. Islam, "Sensor fault and cyber attack resilient operation of dc microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 540–554, 2018.

[62] H. Yan, X. Zhou, H. Zhang, F. Yang, and Z.-G. Wu, "A novel sliding mode estimation for microgrid control with communication time delays," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1509–1520, 2017.

[63] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction

with application to power systems," *IET Control Theory & Applications*, vol. 10, no. 12, pp. 1458–1468, 2016.

[64] G. Rinaldi, P. P. Menon, C. Edwards, A. Ferrara, and Y. Shtessel, "Adaptive dual-layer super-twisting sliding mode observers to reconstruct and mitigate disturbances and communication attacks in power networks," *Automatica*, vol. 129, p. 109656, 2021.

[65] Z. Zhang, Y. Niu, and J. Song, "Input-to-state stabilization of interval type-2 fuzzy systems subject to cyberattacks: An observer-based adaptive sliding mode approach," *IEEE Transactions on Fuzzy Systems*, vol. 28, no. 1, pp. 190–203, 2019.

[66] Q. Su, S. Li, Y. Gao, X. Huang, and J. Li, "Observer-based detection and reconstruction of dynamic load altering attack in smart grid," *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 4013–4027, 2021.

[67] C. Wu, Z. Hu, J. Liu, and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.

[68] L. Ye, F. Zhu, and J. Zhang, "Sensor attack detection and isolation based on sliding mode observer for cyber-physical systems," *International Journal of Adaptive Control and Signal Processing*, vol. 34, no. 4, pp. 469–483, 2020.

[69] V. Utkin, J. Guldner, and J. Shi, *Sliding mode control in electro-mechanical systems*. CRC press, 2017.

[70] G. Chen, Y. Song, and Y. Guan, "Terminal sliding mode-based consensus tracking control for networked uncertain mechanical systems on digraphs," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 3, pp. 749–756, 2016.

[71] M. Lv, W. Yu, Y. Lv, J. Cao, and W. Huang, "An integral sliding mode observer for CPS cyber security attack detection," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 4, p. 043120, 2019.

[72] L. Xu, W. Xiong, M. Zhou, and L. Chen, "A continuous terminal sliding-mode observer-based anomaly detection approach for industrial communication networks," *Symmetry*, vol. 14, no. 1, p. 124, 2022.

[73] H. Wang, H. Jiang, Y. Zhao, H. Guan, B. Hu, and S. Wang, "High-order observer-based sliding mode control for the isolated microgrid with cyber attacks and physical uncertainties," *Complexity*, vol. 2020, 2020.

[74] H. Yang, S. Yin, H. Han, and H. Sun, "Sparse actuator and sensor attacks reconstruction for linear cyber-physical systems with sliding mode observer," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3873–3884, 2021.

[75] M. Li, Y. Chen, Y. Zhang, and Y. Liu, "Adaptive sliding-mode tracking control of networked control systems with false data injection attacks," *Information Sciences*, vol. 585, pp. 194–208, 2022.

[76] L. Chen, C. Edwards, and H. Alwi, "Sensor fault estimation using LPV sliding mode observers with erroneous scheduling parameters," *Automatica*, vol. 101, pp. 66–77, 2019.

[77] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, 2012.

[78] A. J. Abianeh, M. M. Mardani, F. Ferdowsi, R. Gottumukkala, and T. Dragičević, "Cyber-resilient sliding-mode consensus secondary control scheme for islanded ac microgrids," *IEEE Transactions on Power Electronics*, vol. 37, no. 5, pp. 6074–6089, 2021.

[79] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1953–1963, 2021.

[80] X. Li, Q. Xu, and F. Blaabjerg, "Adaptive resilient secondary control for islanded ac microgrids with sensor faults," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5239–5248, 2020.

[81] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73–77, 2020.

[82] A. Afshari, M. Karrari, H. R. Baghaee, and G. Gharehpetian, "Resilient synchronization of voltage/frequency in ac microgrids under deception attacks," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2125–2136, 2020.

[83] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3728–3741, 2020.

[84] B. P. Poudel, A. Mustafa, A. Bidram, and H. Modares, "Detection and mitigation of cyber-threats in the dc microgrid distributed control system," *International Journal of Electrical Power & Energy Systems*, vol. 120, p. 105968, 2020.

[85] Y. Yamamoto, N. Kuze, and T. Ushio, "Attack detection and defense system using an unknown input observer for cooperative adaptive cruise control systems," *IEEE Access*, vol. 9, pp. 148 810–148 820, 2021.

[86] X. Wang, X. Luo, X. Pan, and X. Guan, "Detection and location of bias load injection attack in smart grid via robust adaptive observer," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4454–4465, 2020.

[87] H. Shafei, L. L. A. R. P. Farhangi, Majid, H. H. Alhelou *et al.*, "A novel cyber-attack detection and mitigation for coupled power and information networks in microgrids using distributed sliding mode unknown input observer," *IEEE Transactions on Smart Grid*, 2024.

[88] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[89] A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, "Novel SMO-based detection and isolation of false data injection attacks against frequency control systems," *IEEE Transactions on Power Systems*, 2023.

[90] Y. Liu, T. Li, B.-C. Zheng, and M. Shen, "Distributed resilient state estimation for nonlinear systems against sensor attacks," *IEEE Transactions on Industrial Informatics*, 2023.

[91] H. Shafei, L. Li, and R. P. Aguilera, "Observer-based attack detection and mitigation in dc microgrid systems," in *2023 IEEE 14th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*. IEEE, 2023, pp. 959–964.

[92] J. Yan, F. Guo, and C. Wen, "Attack detection and isolation for distributed load shedding algorithm in microgrid systems," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 1, no. 1, pp. 102–110, 2020.

[93] X. Wang, X. Luo, M. Zhang, Z. Jiang, and X. Guan, "Detection and localization of biased load attacks in smart grids via interval observer," *Information Sciences*, vol. 552, pp. 291–309, 2021.

[94] X. Luo, X. Wang, X. Pan, and X. Guan, "Detection and isolation of false data injection attack for smart grids via unknown input observers," *IET Generation, Transmission & Distribution*, vol. 13, no. 8, pp. 1277–1286, 2019.

[95] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3984–3996, 2021.

[96] Y. Zhao, C. Zhou, Y.-C. Tian, and Y. Qin, "Composite finite-time resilient control for cyber-physical systems subject to actuator attacks," *IEEE transactions on cybernetics*, vol. 53, no. 2, pp. 1063–1077, 2021.

[97] M. Liu, X. Zhang, R. Zhang, Z. Zhou, Z. Zhang, and R. Deng, "Detection-triggered recursive impact mitigation against secondary false data injection attacks in cyber-physical microgrids," *IEEE Transactions on Control of Network Systems*, vol. 16, no. 2, pp. 1744–1761, 2025.

[98] M. Liu, C. Zhao, R. Deng, P. Cheng, and J. Chen, "False data injection attacks and the distributed countermeasure in dc microgrids," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 4, pp. 1962–1974, 2022.

[99] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, "Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1162–1169, 2018.

[100] Y. Mao, H. Jafarnejadsani, P. Zhao, E. Akyol, and N. Hovakimyan, "Novel stealthy attack and defense strategies for networked control systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3847–3862, 2020.

[101] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2019.

[102] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[103] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy," *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3714–3721, 2019.

[104] S. Nateghi, Y. Shtessel, and C. Edwards, "Cyber-attacks and faults reconstruction using finite time convergent observation algorithms: Electric power network application," *Journal of the Franklin Institute*, vol. 357, no. 1, pp. 179–205, 2020.

[105] Y. Li, H. Fang, and J. Chen, "Anomaly detection and identification for multiagent systems subjected to physical faults and cyberattacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 11, pp. 9724–9733, 2019.

[106] D. Das, S. Madichetty, B. Singh, and S. Mishra, "Luenberger observer based current estimated boost converter for PV maximum power extraction—a current sensorless approach," *IEEE Journal of Photovoltaics*, vol. 9, no. 1, pp. 278–286, 2018.

[107] R. Gao, J. Huang, X. Su, and L. Zhao, "K-filter-based adaptive output feedback control for high-order nonlinear systems subject to actuator and sensor attacks," *International Journal of Robust and Nonlinear Control*, vol. 32, no. 6, pp. 3469–3484, 2022.

[108] J.-J. Yan, G.-H. Yang, and Y. Wang, "Dynamic reduced-order observer-based detection of false data injection attacks with application to smart grid systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 6712–6722, 2022.

[109] L. An and G.-H. Yang, "Supervisory nonlinear state observers for adversarial sparse attacks," *IEEE Transactions on Cybernetics*, 2020.

[110] J. Yang, W.-A. Zhang, and F. Guo, "Adaptive distributed Kalman-like filter for power system with cyber attacks," *Automatica*, vol. 137, p. 110091, 2022.

[111] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers & Security*, vol. 89, p. 101677, 2020.

[112] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, 2015.

[113] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2020.

[114] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in dc microgrids," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1487–1498, 2021.

[115] S. Zhao, F. Blaabjerg, and H. Wang, "An overview of artificial intelligence applications for power electronics," *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4633–4658, 2020.

[116] Y. Wan and T. Dragicevic, "Data-driven cyber-attack detection of intelligent attacks in islanded dc microgrids," *IEEE Transactions on Industrial Electronics*, 2022.

[117] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[118] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2019, pp. 1–6.

[119] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in *2017 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2017, pp. 3854–3861.

[120] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31 711–31 722, 2019.

[121] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[122] K. Sethi, R. Kumar, N. Prajapati, and P. Bera, "Deep reinforcement learning based intrusion detection system for cloud infrastructure," in *2020 International Conference on Communication Systems & Networks (COMSNETS)*. IEEE, 2020, pp. 1–6.

[123] M. G. Raman, N. Somu, K. Kirthivasan, R. Liscano, and V. S. Sriram, "An efficient intrusion detection system based on hypergraph-genetic algorithm for parameter optimization and feature selection in support vector machine," *Knowledge-Based Systems*, vol. 134, pp. 1–12, 2017.

[124] X. Ma, L. Yang, L. Ma, W. Dong, M. Jin, L. Zhang, F. Yang, and Y. Lin, "Consensus tracking control for uncertain non-strict feedback multi-agent system under cyber attack via resilient neuroadaptive approach," *International Journal of Robust and Nonlinear Control*, vol. 32, no. 7, pp. 4251–4280, 2022.

[125] G. B. Gaggero, R. Caviglia, A. Armellin, M. Rossi, P. Girdinio, and M. Marchese, "Detecting cyberattacks on electrical storage systems through neural network based anomaly detection algorithm," *Sensors*, vol. 22, no. 10, p. 3933, 2022.

[126] M. Mohammadpourfard, A. Sami, and A. R. Seifi, "A statistical unsupervised method against false data injection attacks: A visualization-based approach," *Expert Systems with Applications*, vol. 84, pp. 242–261, 2017.

[127] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, "Decentralized coordinated cyberattack detection and mitigation strategy in dc microgrids based on artificial neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4629–4638, 2021.

[128] K. Hughes, K. McLaughlin, and S. Sezer, "A model-free approach to intrusion response systems," *Journal of Information Security and Applications*, vol. 66, p. 103150, 2022.

[129] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2020.

[130] M. Dehghani, T. Niknam, M. Ghiasi, N. Bayati, and M. Savaghebi, "Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach," *Electronics*, vol. 10, no. 16, p. 1914, 2021.

[131] X. Gao, C. Hu, C. Shan, B. Liu, Z. Niu, and H. Xie, "Malware classification for the cloud via semi-supervised transfer learning," *Journal of Information Security and Applications*, vol. 55, p. 102661, 2020.

[132] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 375–386, 2021.

[133] M. Shafiee-Rad, M. S. Sadabadi, Q. Shafiee, and M. R. Jahed-Motlagh, "Robust decentralized voltage control for uncertain dc microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 125, p. 106468, 2021.

[134] Y. Barzegari, J. Zarei, R. Razavi-Far, M. Saif, and V. Palade, "Resilient consensus control design for dc microgrids against false data injection attacks using a distributed bank of sliding mode observers," *Sensors*, vol. 22, no. 7, p. 2644, 2022.

[135] S. Zuo, Y. Zhang, and Y. Wang, "Adaptive resilient control of ac microgrids under unbounded actuator attacks," *Energies*, vol. 15, no. 20, p. 7458, 2022.

[136] B. E. Sedhom, A. Y. Hatata, M. M. El-Saadawi, and E.-H. E. Abd-Raboh, "Robust adaptive H_∞ based controller for islanded microgrid supplying non-linear and unbalanced loads," *IET Smart Grid*, vol. 2, no. 3, pp. 420–435, 2019.

[137] D. K. Mishra, P. K. Ray, L. Li, J. Zhang, M. Hossain, and A. Mohanty, "Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties," *Applied Energy*, vol. 306, p. 118054, 2022.

[138] Y. Seyedi, H. Karimi, and J. Mahseredjian, "A data-driven method for prediction of post-fault voltage stability in hybrid ac/dc microgrids," *IEEE Transactions on Power Systems*, 2022.

[139] J. Duan, W. Zeng, and M.-Y. Chow, "Resilient distributed dc optimal power flow against data integrity attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2016.

[140] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543–1551, 2018.

[141] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017.

[142] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.

[143] L. Ding, Q.-L. Han, B. Ning, and D. Yue, "Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4909–4919, 2019.

[144] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial informatics*, vol. 16, no. 6, pp. 3881–3894, 2019.

[145] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed resilient control for energy storage systems in cyber-physical microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1331–1341, 2020.

[146] T. Ding, Y. Lin, Z. Bie, and C. Chen, "A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration," *Applied Energy*, vol. 199, pp. 205–216, 2017.

[147] H. R. Baghaee, M. Mirsalim, G. B. Gharehpetian, and H. A. Talebi, "A decentralized robust mixed H_2/H_∞ voltage control scheme to improve small/large-signal stability and FRT capability of islanded multi-DER microgrid considering load disturbances," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2610–2621, 2017.

[148] X. Li, C. Wen, C. Chen, and Q. Xu, "Adaptive resilient secondary control for microgrids with communication faults," *IEEE Transactions on Cybernetics*, 2021.

[149] Y. Zhao, X. Du, C. Zhou, Y.-C. Tian, X. Hu, and D. E. Quevedo, "Adaptive resilient control of cyber-physical systems under actuator and sensor attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3203–3212, 2021.

[150] C. Deng, D. Zhang, and G. Feng, "Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks," *Automatica*, vol. 139, p. 110172, 2022.

[151] P. Meng, W. Xiang, Y. Chi, Z. Wang, W. Lin, and J. Wen, "Resilient dc voltage control for islanded wind farms integration using cascaded hybrid HVDC system," *IEEE Transactions on Power Systems*, vol. 37, no. 2, pp. 1054–1066, 2021.

[152] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability-oriented design of cyberattack-resilient controllers for cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 37, no. 2, pp.

1310–1321, 2021.

[153] S. Saha, S. Gholami, and M. K. K. Prince, "Sensor fault-resilient control of electronically coupled distributed energy resources in islanded microgrids," *IEEE Transactions on Industry Applications*, vol. 58, no. 1, pp. 914–929, 2021.

[154] Y. Shan, A. Pan, and H. Liu, "A switching event-triggered resilient control scheme for primary and secondary levels in ac microgrids," *ISA Transactions*, 2022.

[155] T. Vigneysh, N. Pachauri, and V. Suresh, "Internal model-based cascaded control approach for multi-functional grid interactive converters," *IEEE Access*, vol. 10, pp. 19 862–19 874, 2022.

[156] M. I. Ibraheem, M. Edrisi, H. H. Alhelou, M. Gholipour, and A. Al-Hinai, "A sophisticated slide mode controller of microgrid system load frequency control under false data injection attack and actuator time delay," *IEEE Transactions on Industry Applications*, vol. 60, no. 2, pp. 2117–2126, 2023.

[157] K. Wan, J. Zhao, Y. Chen, and M. Yu, "A decentralized resilient control scheme for dc microgrids against faults on sensor and actuator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 71, no. 2, pp. 816–827, 2023.

[158] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. R. Hui, "A high-order differentiator based distributed secondary control for dc microgrids against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 4035–4045, 2021.

[159] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, "Distributed sliding mode observer-based secondary control for dc microgrids under cyber-attacks," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 144–154, 2020.

[160] M. Kachhwaha, H. Modi, M. K. Nehra, and D. Fulwani, "Resilient control of dc microgrids against cyber attacks: A functional observer based approach," *IEEE Transactions on Power Electronics*, 2023.

[161] M. A. Taher, M. Tariq, M. Behnamfar, and A. I. Sarwat, "Analyzing replay attack impact in dc microgrid consensus control: Detection and mitigation by Kalman-filter-based observer," *IEEE Access*, vol. 11, pp. 121 368–121 378, 2023.

[162] D. Zhou, Q. Zhang, F. Guo, Z. Lian, J. Qi, and W. Zhou, "Distributed resilient secondary control for islanded dc microgrids considering unbounded FDI attacks," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 160–170, 2023.

[163] J.-J. Yan and G.-H. Yang, "Secure state estimation of nonlinear cyber-physical systems against DoS attacks: A multiobserver approach," *IEEE Transactions on Cybernetics*, vol. 53, no. 3, pp. 1447–1459, 2021.

[164] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2020.

[165] X. Chen, J. Zhou, M. Shi, Y. Chen, and J. Wen, "Distributed resilient control against denial of service attacks in dc microgrids with constant power load," *Renewable and Sustainable Energy Reviews*, vol. 153, p. 111792, 2022.

[166] S. Song, B. Zhang, J. H. Park, and X. Song, "Adaptive resilient control design for nonlinear time-delay systems against unknown state-dependent deception attacks," *International Journal of Robust and Nonlinear Control*, vol. 32, no. 4, pp. 2159–2182, 2022.

[167] C. Edwards and S. Spurgeon, *Sliding mode control: theory and applications*. CRC Press, 1998.

[168] M. Corless and J. Tu, "State and input estimation for a class of uncertain systems," *Automatica*, vol. 34, no. 6, pp. 757–764, 1998.

[169] S. Andrilli and D. Hecker, *Elementary linear algebra*. Academic Press, 2022.

[170] J. Gallier *et al.*, "The schur complement and symmetric positive semidefinite (and definite) matrices (2019)," *URL https://www. cis. upenn. edu/jean/schur-comp. pdf*, 2020.

[171] G. A. Seber and A. J. Lee, *Linear regression analysis*. John Wiley & Sons, 2003, vol. 330.

[172] S. Sen and V. Kumar, "Microgrid control: A comprehensive survey," *Annual Reviews in Control*, vol. 45, pp. 118–151, 2018.

[173] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, "Stable current sharing and voltage balancing in dc microgrids: A consensus-based secondary control layer," *Automatica*, vol. 95, pp. 1–13, 2018.

[174] S. Trip, M. Cucuzzella, C. De Persis, X. Cheng, and A. Ferrara, "Sliding modes for voltage regulation and current sharing in dc microgrids," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 6778–6783.

[175] D.-J. Lee, Y. Park, and Y.-s. Park, "Robust sliding mode descriptor observer for fault and output disturbance estimation of uncertain systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 11, pp. 2928–2934, 2012.

[176] L. Xu, Y. Chen, and M. Li, "Sliding mode resilient control for TOD-based servo system under DoS attack," *International Journal of Control, Automation and Systems*, vol. 20, no. 2, pp. 526–535, 2022.

[177] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2017.

[178] M. Tucci, S. Riverso, J. C. Vasquez, J. M. Guerrero, and G. Ferrari-Trecate, "A decentralized scalable approach to voltage control of dc islanded microgrids," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 6, pp. 1965–1979, 2016.

[179] M. Tucci, S. Riverso, and G. Ferrari-Trecate, "Line-independent plug-and-play controllers for voltage stabilization in dc microgrids," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 3, pp. 1115–1123, 2017.

[180] D. S. Bernstein, *Matrix mathematics: theory, facts, and formulas*. Princeton university press, 2009.

[181] B. Alenezi, M. Zhang, S. Hui, and S. H. Żak, "Simultaneous estimation of the state, unknown input, and output disturbance in discrete-time linear systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 12, pp. 6115–6122, 2021.

[182] T. N. E. Greville, "Note on the generalized inverse of a matrix product," *SIAM Review*, vol. 8, no. 4, pp. 518–521, 1966.

[183] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[184] S. Rath, D. Pal, P. S. Sharma, and B. K. Panigrahi, "A cyber-secure distributed control architecture for autonomous ac microgrid," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3324–3335, 2020.

[185] X. Luo, Y. Li, X. Wang, and X. Guan, "Interval observer-based detection and localization against false data injection attack in smart grids," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 657–671, 2020.

[186] J. Callenes and M. Poshtan, "Dynamic reconfiguration for resilient state estimation against cyber attacks," *IEEE Transactions on Emerging Topics in Computing*, 2023.

[187] R. Lu, J. Wang, and Z. Wang, "Distributed observer-based finite-time control of ac microgrid under attack," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 157–168, 2020.

[188] M. Cucuzzella, G. P. Incremona, and A. Ferrara, "Decentralized sliding mode control of islanded ac microgrids with arbitrary topology," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 8, pp. 6706–6713, 2017.

[189] T. Huang, D. Wu, and M. Ilić, "Cyber-resilient automatic generation control for systems of ac microgrids," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 886–898, 2023.